Exploitation Of Windows .NET Framework

Nanika

nanika_pan@trend.com.tw

I am Nanika
Black Hat
our Media
BEYOND security
CHROOT
CLUSIF
EWF Executive Women's Forum

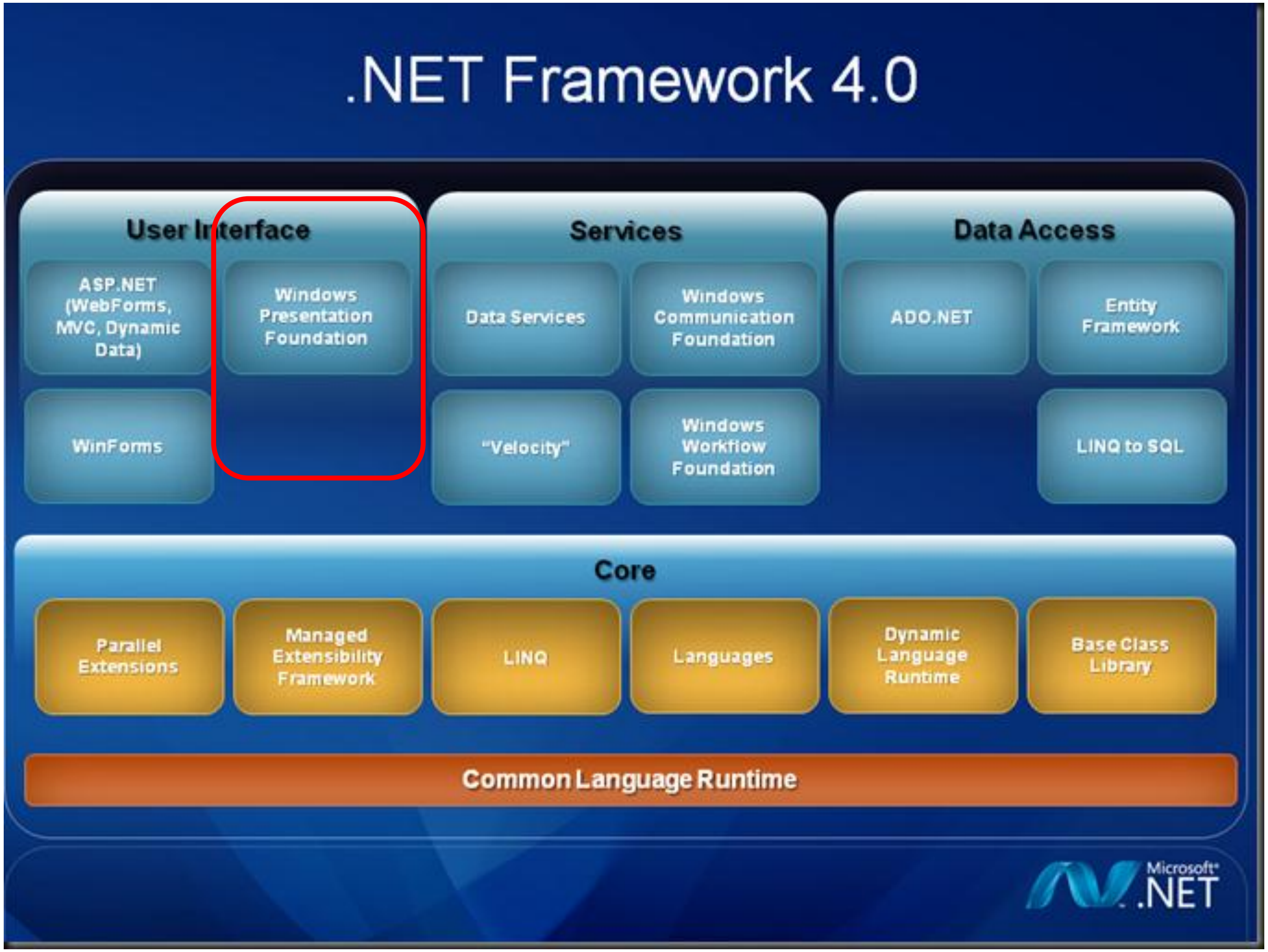
.NET Framework

- APT ?
- No Exploit in .NET?
- Only EXE Attack?

- TREND MICRO always Finds the New Attack TREND
- 趨勢始終來自於弱點

.Net framework Security Improvements

.NET Architecture



.NET Framework 4.0

User Interface

- ASP.NET (WebForms, MVC, Dynamic Data)
- Windows Presentation Foundation
- WinForms

Services

- Data Services
- Windows Communication Foundation
- "Velocity"
- Windows Workflow Foundation

Data Access

- ADO.NET
- Entity Framework
- LINQ to SQL

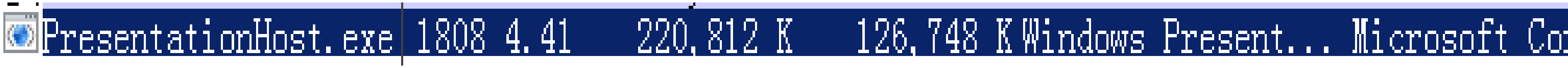
Core

- Parallel Extensions
- Managed Extensibility Framework
- LINQ
- Languages
- Dynamic Language Runtime
- Base Class Library

Common Language Runtime

WPF

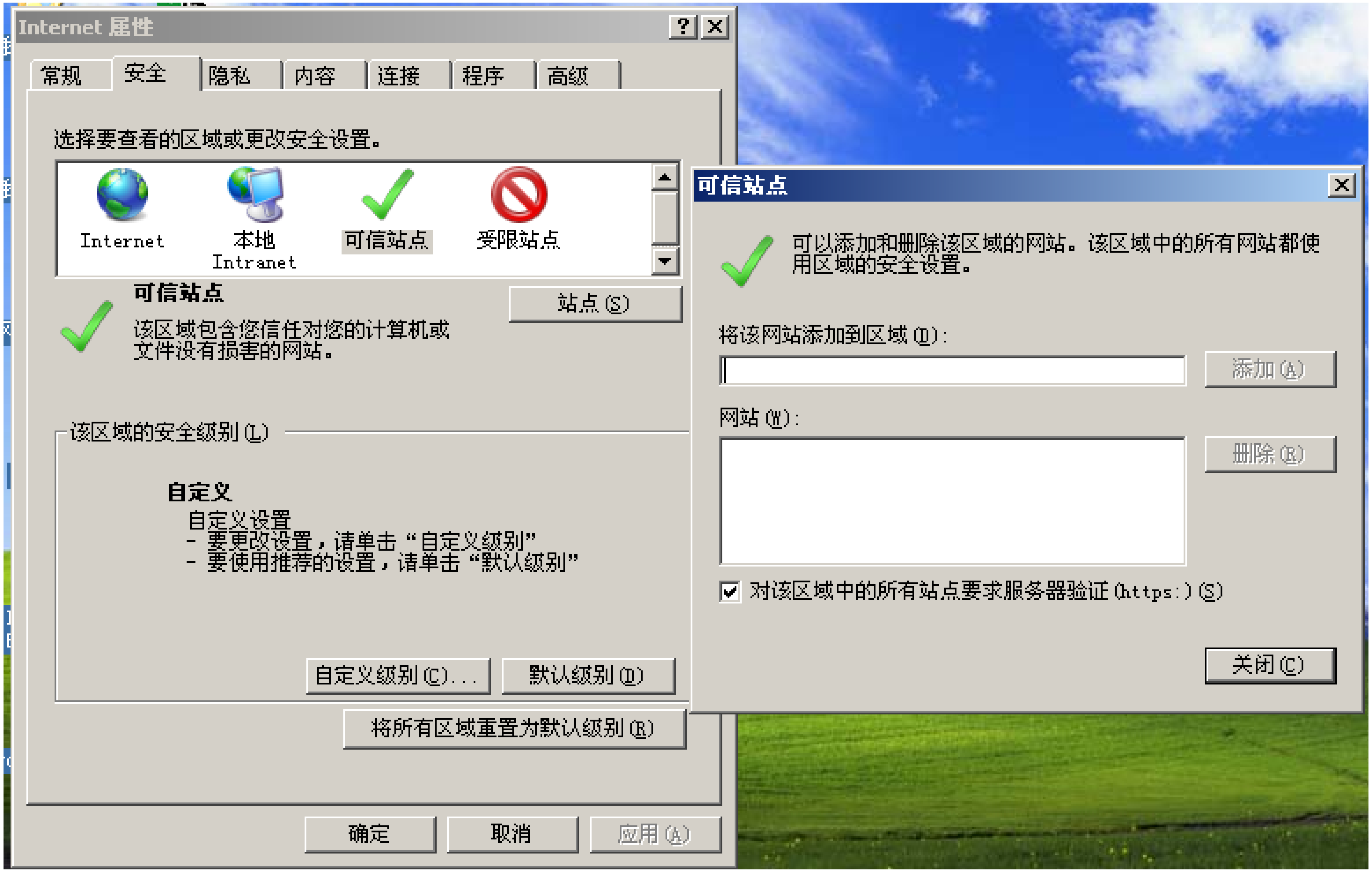
- Windows Presentation Foundation (WPF) browser-hosted applications
- Default Enable DEP



```
PresentationHost.exe  1808 4.41    220,812 K    126,748 K Windows Present... Microsoft Co
```

Security Zone	Behavior	Getting Full Trust
Local computer	Automatic full trust	No action is needed.
Intranet and trusted sites	Prompt for full trust	Sign the XBAP with a certificate so that the user sees the source in the prompt.
Internet	Fails with "Trust Not Granted"	Sign the XBAP with a certificate.

Trust Site



选择要查看的区域或更改安全设置。

可信站点

该区域包含您信任对您的计算机或文件没有损害的网站。

该区域的安全级别(L)

自定义

自定义设置
- 要更改设置，请单击“自定义级别”
- 要使用推荐的设置，请单击“默认级别”

可以添加和删除该区域的网站。该区域中的所有网站都使用区域的安全设置。

将该网站添加到区域(D):

网站(W):

☑ 对该区域中的所有站点要求服务器验证(https:)(S)

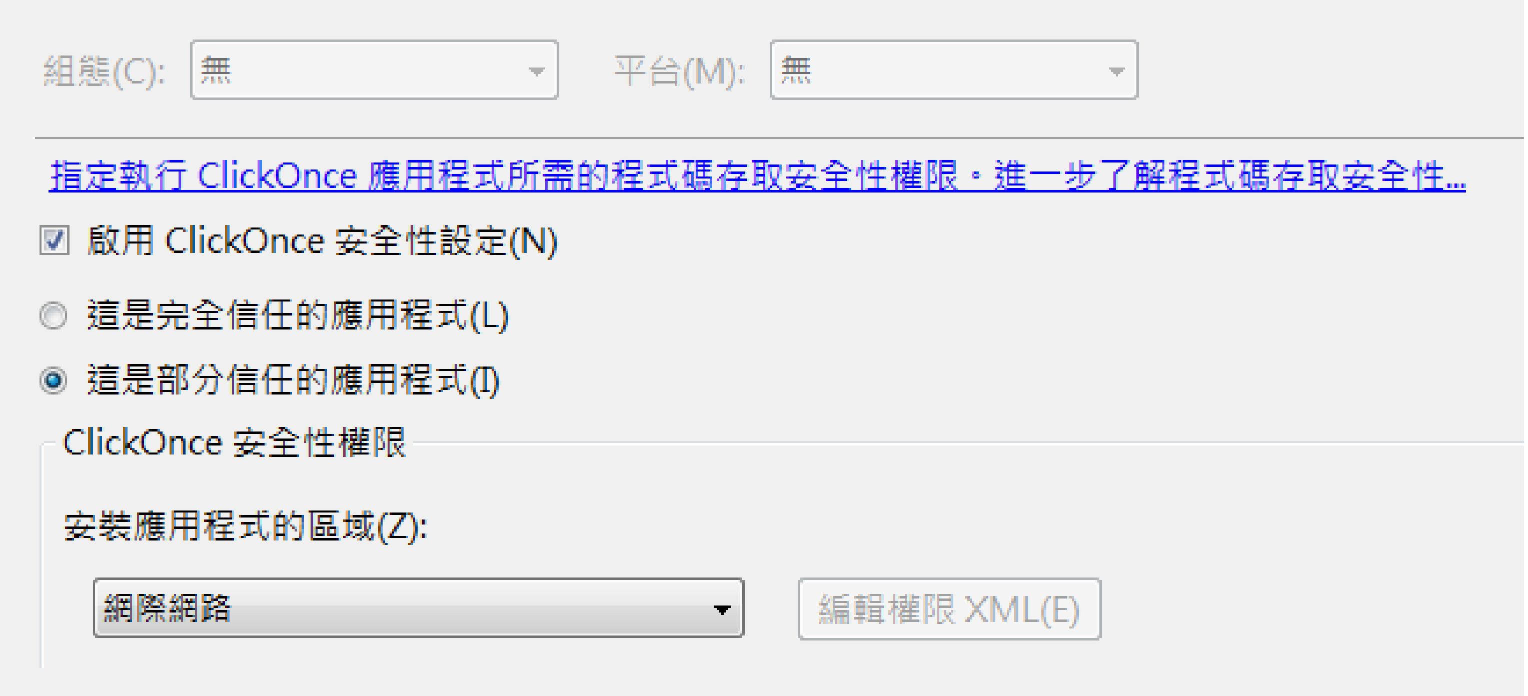
Debug WPF

- To configure Microsoft Visual Studio 2005 to debug an XBAP that calls a Web service:
- With a project selected in **Solution Explorer**, on the **Project** menu, click **Properties**.
- In the **Project Designer**, click the **Debug** tab.
- In the **Start Action** section, select **Start external program** and enter the following:
- C:\WINDOWS\System32\PresentationHost.exe
- In the **Start Options** section, enter the following into the **Command line arguments** text box:
- -debug *filename*
- The *filename* value for the **-debug** parameter is the .xbap filename; for example:
- -debug c:\example.xbap

ClickOnce Deployment

Task	ClickOnce	Windows Installer
Install Files	**X**	**X**
Create Shortcuts	**X**	**X**
Associate File Extensions	**X**	**X**
Install Services		**X**
Install to GAC		**X**
Manage ODBC		**X**
Manage COM+		**X**
Write to Registry		**X**
Advertising		**X**
Self-Repair		**X**
File/Folder/Registry Permissions		**X**

ClickOnce INTERNET or Full Trust



組態(C): 無

平台(M): 無

指定執行 ClickOnce 應用程式所需的程式碼存取安全性權限。進一步了解程式碼存取安全性...

☑ 啟用 ClickOnce 安全性設定(N)

○ 這是完全信任的應用程式(L)

● 這是部分信任的應用程式(I)

ClickOnce 安全性權限

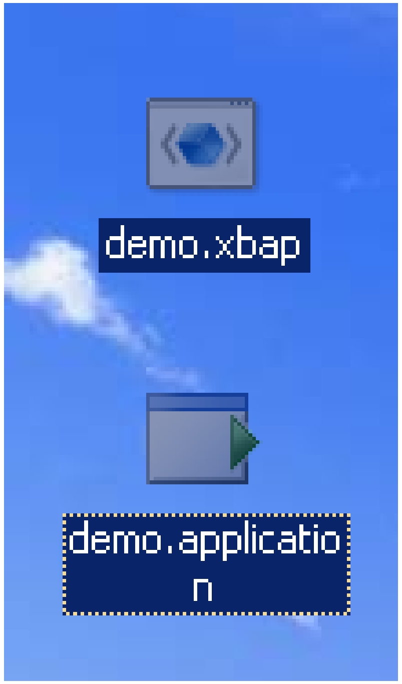
安裝應用程式的區域(Z): 網際網路

Examples of permissions not available in the Internet zone

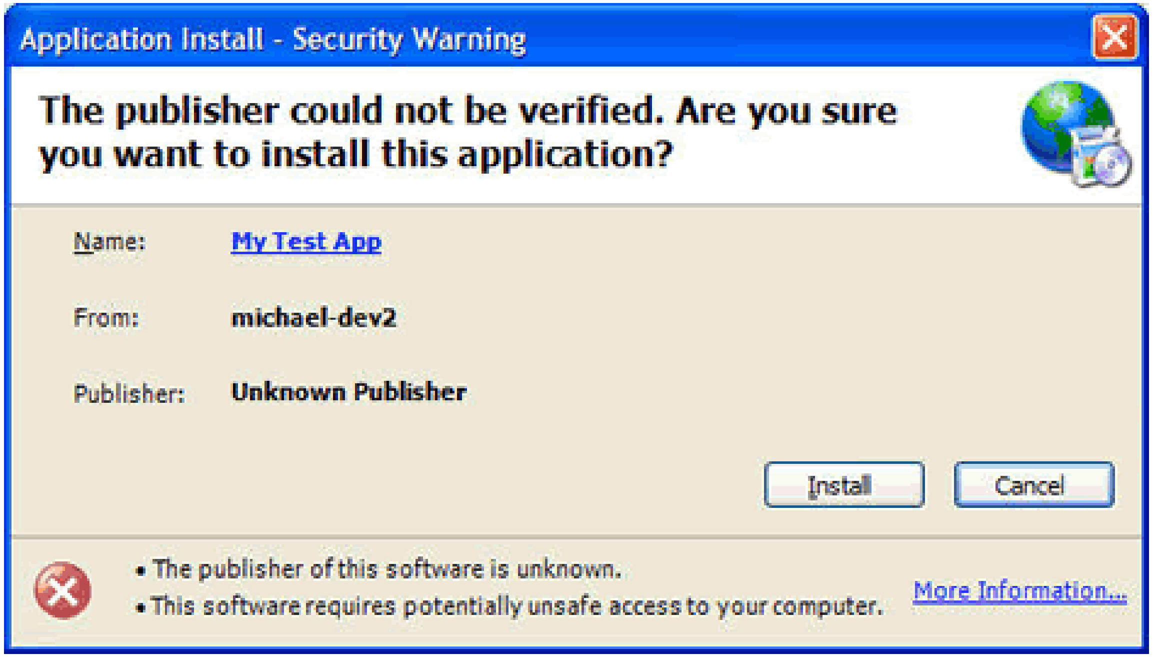
FileIOPermission	This permission controls the ability to read and write files on disk. Consequently, applications in the Internet zone cannot read files on the user's hard disk.
RegistryPermission	This permission controls the ability to read/write to the registry. Consequently, applications in the Internet zone cannot access or control state in the user's registry.
SecurityPermission.UnmanagedCode	This permission controls the ability to call native Win32 functions.

http://msdn.microsoft.com/en-us/library/aa480229.aspx

.XBAP/.Application



Warring



Application Install - Security Warning

The publisher could not be verified. Are you sure you want to install this application?

Name: My Test App

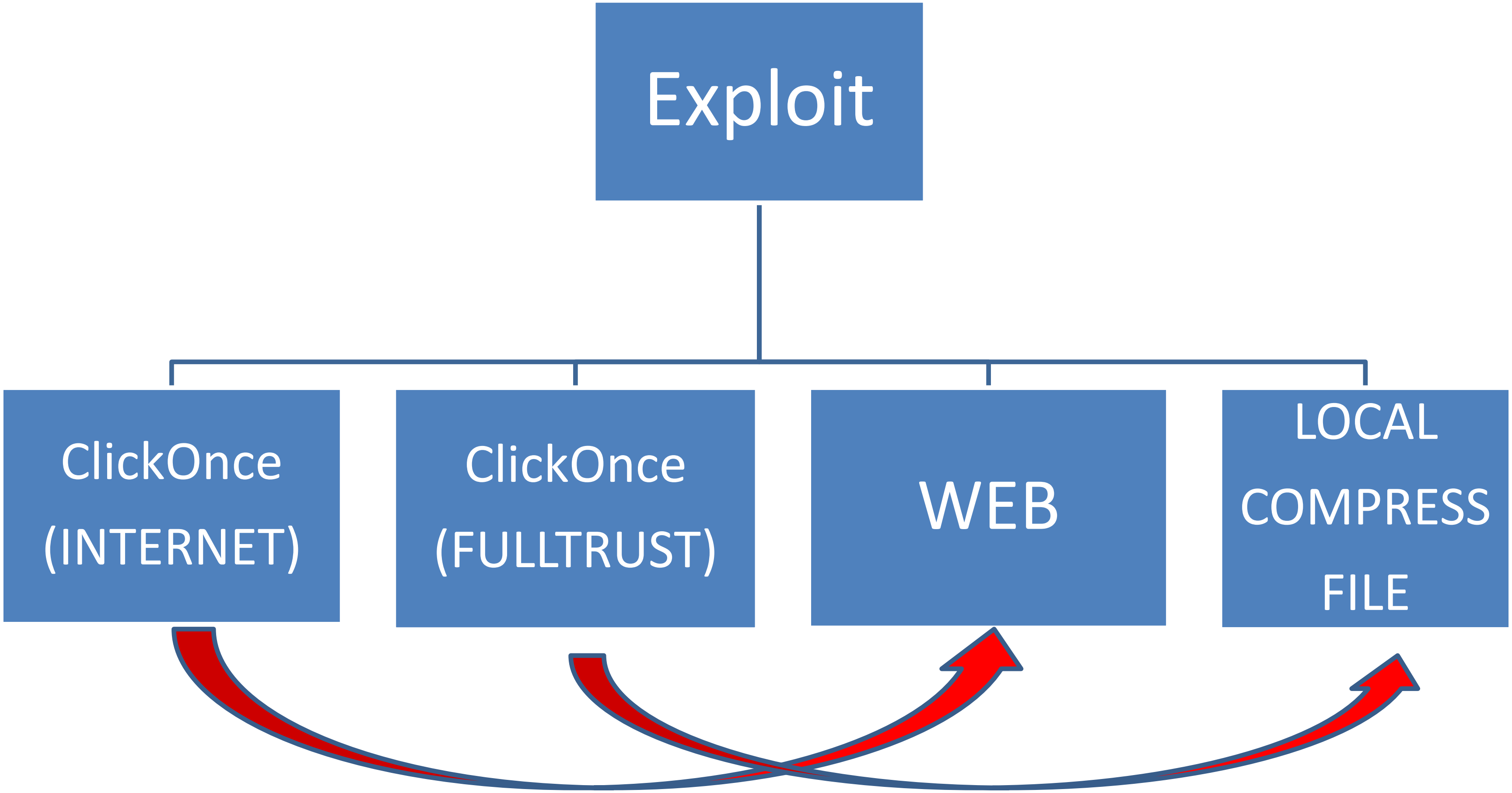
From: michael-dev2

Publisher: Unknown Publisher

- The publisher of this software is unknown.
- This software requires potentially unsafe access to your computer.

- .NET framework

Start the exploitation



Exploit

ClickOnce (INTERNET)

ClickOnce (FULLTRUST)

WEB

LOCAL COMPRESS FILE

ClickOnce (INTERNET)+WEB with MS12-035

- 00000025 mov   eax,dword ptr ds:[037B20C4h]
- 0000002b mov   dword ptr [ebp-40h],eax
- 0000002e mov   ecx,dword ptr [ebp-3Ch]//ecx=0x41414141
- 00000031 mov   eax,dword ptr [ecx]
- 00000033 mov   eax,dword ptr [eax+28h]
- 00000036 call   dword ptr [eax]

Exploit

- byte[] proc = new byte[] {
- EIP,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- 0x0d, 0x0d, 0x0d, 0x0d,
- Proc point,
- 0x0d, 0x0d, 0x0d, 0x0d,

.NET Native API Alloc (full trust)

- [DllImport("kernel32")]
- private static extern UInt32 VirtualAlloc(UInt32 lpStartAddr,UInt32 size, UInt32 flAllocationType, UInt32 flProtect);
- UInt32 exec = VirtualAlloc(0, (UInt32)proc.Length, 0x1000, 0x40);
- byte[] byteArrays = BitConverter.GetBytes(exec);

.NET Alloc (full trust)

- int sz = 0x1000;
- IntPtr ptr = Marshal.AllocHGlobal(sz);
- uint exec = (uint)ptr.ToInt32();
- byte[] byteArrays = BitConverter.GetBytes(exec);

Byte[] to uint (full trust)

```
•  unsafe
•                  {
•                     fixed (byte* p = proc)
•                     {
•                        IntPtr ptr = (IntPtr)p;
•                      }
•                  }
```

GCHandle.Alloc (full trust)

- GCHandle pinnedArray = GCHandle.Alloc(proc, GCHandleType.Pinned);
- IntPtr pointer = pinnedArray.AddrOfPinnedObject();
- pinnedArray.Free();

Exploit MS12-035

- Heap spraying
- Find no ASLR module
- ROP
- Run Shellcode
- Use COM technical bypass HIPS(blackhat 2011)

- Demo

Attack (ClickOnce INTERNET)

- .NET limit by Windows Presentation Foundation Security Sandbox
- .XBAP
- .Applacation
- html

Local Compress File Attack

Internet Attack ~~mush add trust site~~ no warning

Why AntiVirus can not Detect?

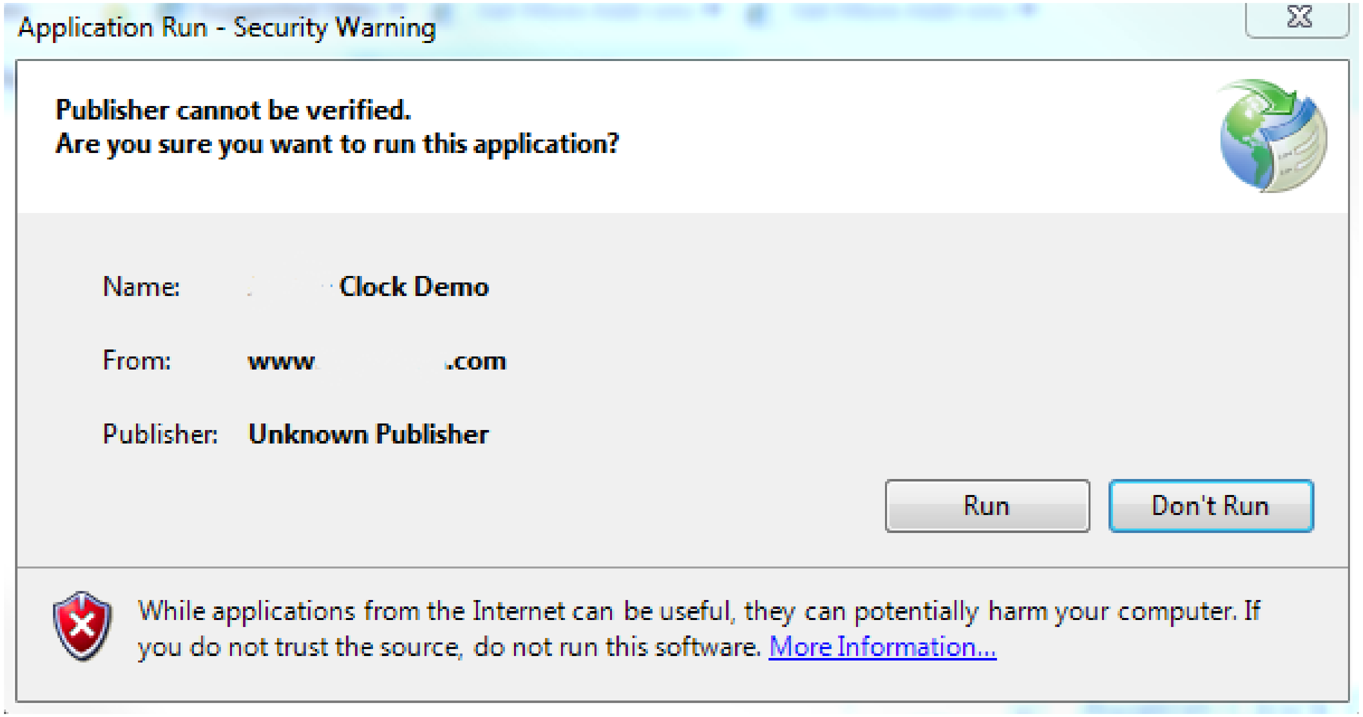
- ALL AV Focus in Internet Explore Process
- The Heap Spraying Detect only in Browser Process
- The Script Decode not work in WPF process
- Static Detect XBAP ?

Patched Affect

- MS11-044 INTERNET check
- MS12-035 INTERNET and LOCAL check

Remote Attack on MS11-044

- Web Attack Demo



Application Run - Security Warning

Publisher cannot be verified.
Are you sure you want to run this application?

Name: **Clock Demo**

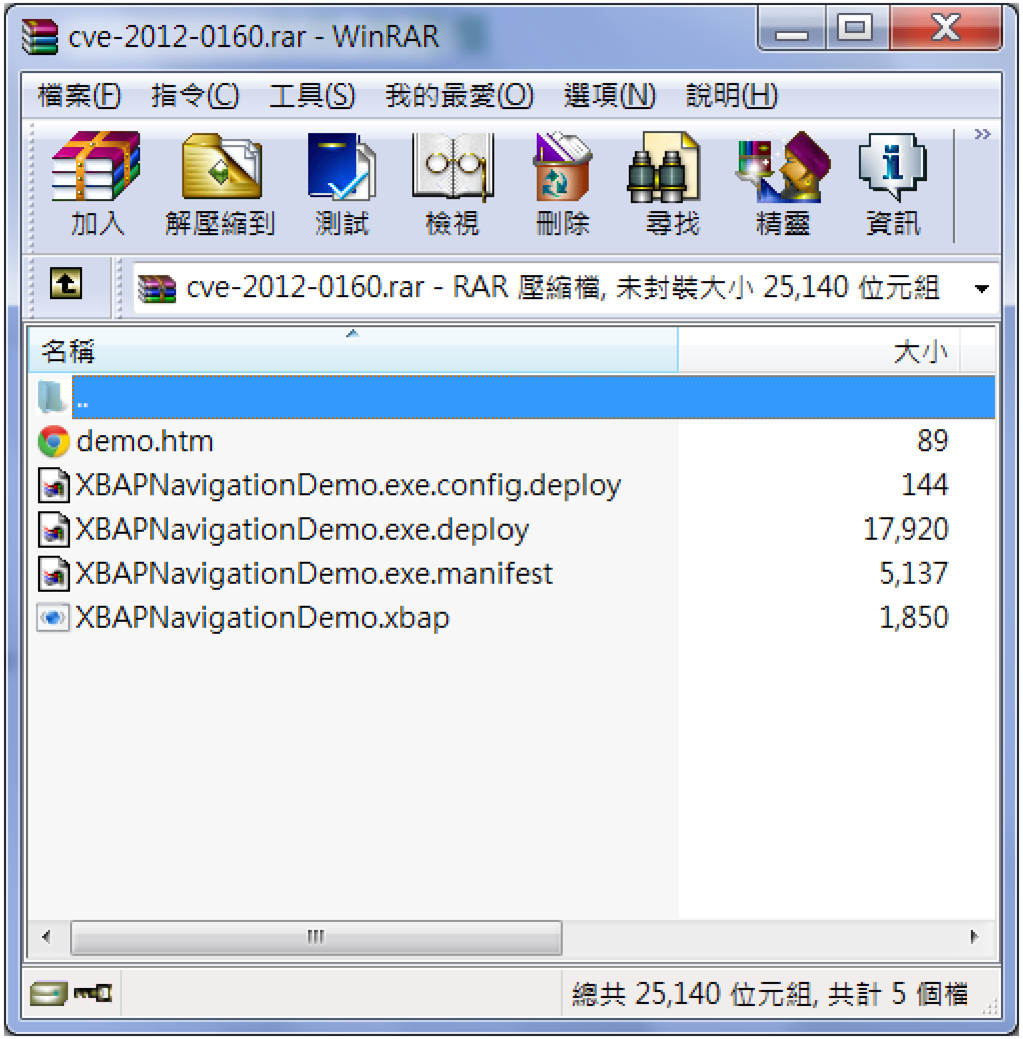
From: **www .com**

Publisher: **Unknown Publisher**

While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not run this software. More Information...

Patched MS11-044 Attack bypass

- LocalComputer
- RAR



cve-2012-0160.rar - RAR 壓縮檔, 未封裝大小 25,140 位元組

名稱	大小
..	
demo.htm	89
XBAPNavigationDemo.exe.config.deploy	144
XBAPNavigationDemo.exe.deploy	17,920
XBAPNavigationDemo.exe.manifest	5,137
XBAPNavigationDemo.xbap	1,850

總共 25,140 位元組, 共計 5 個檔

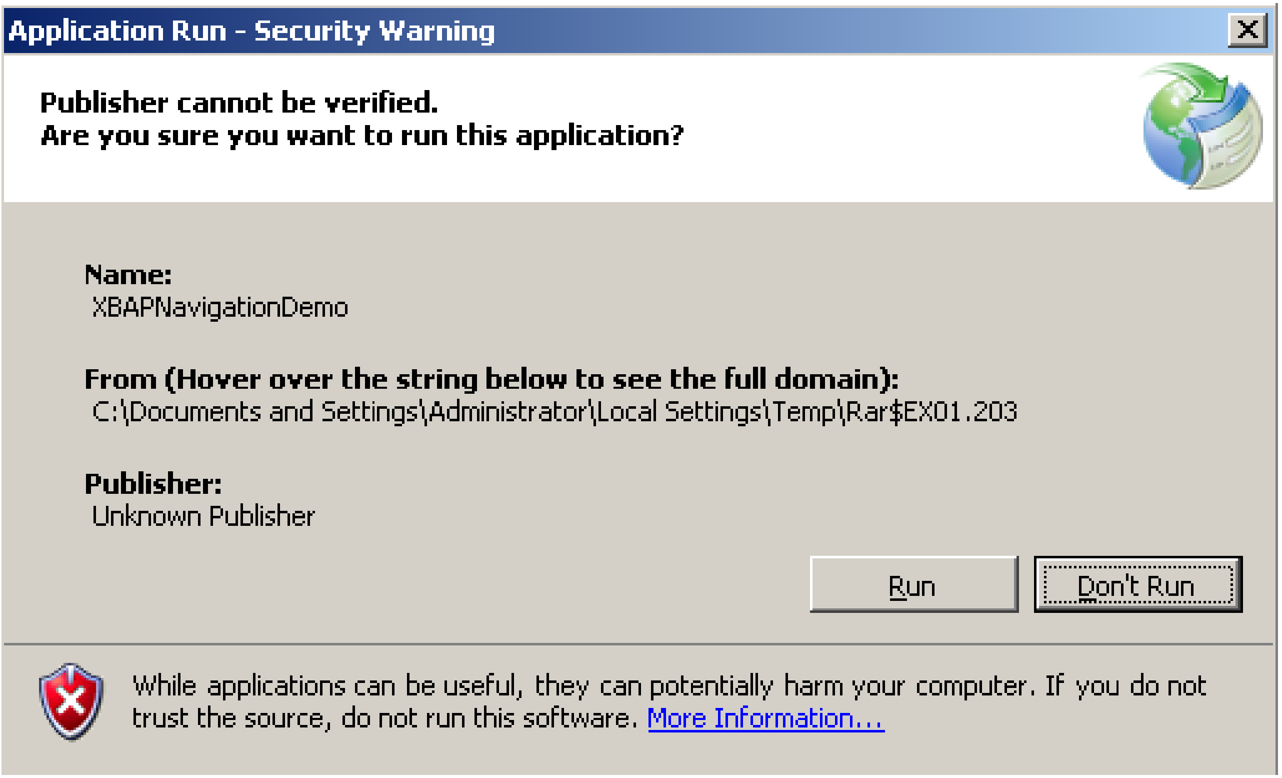
Attack (ClickOnce FULL TRUST)

- .NET can control everything
- .XBAP
- .Applacation
- Html
- Process.Start(“calc.exe”);

WEB Attack mush add trust site and warning

MS12-035

- Local Warning



Application Run - Security Warning

Publisher cannot be verified.
Are you sure you want to run this application?

Name:
XBAPNavigationDemo

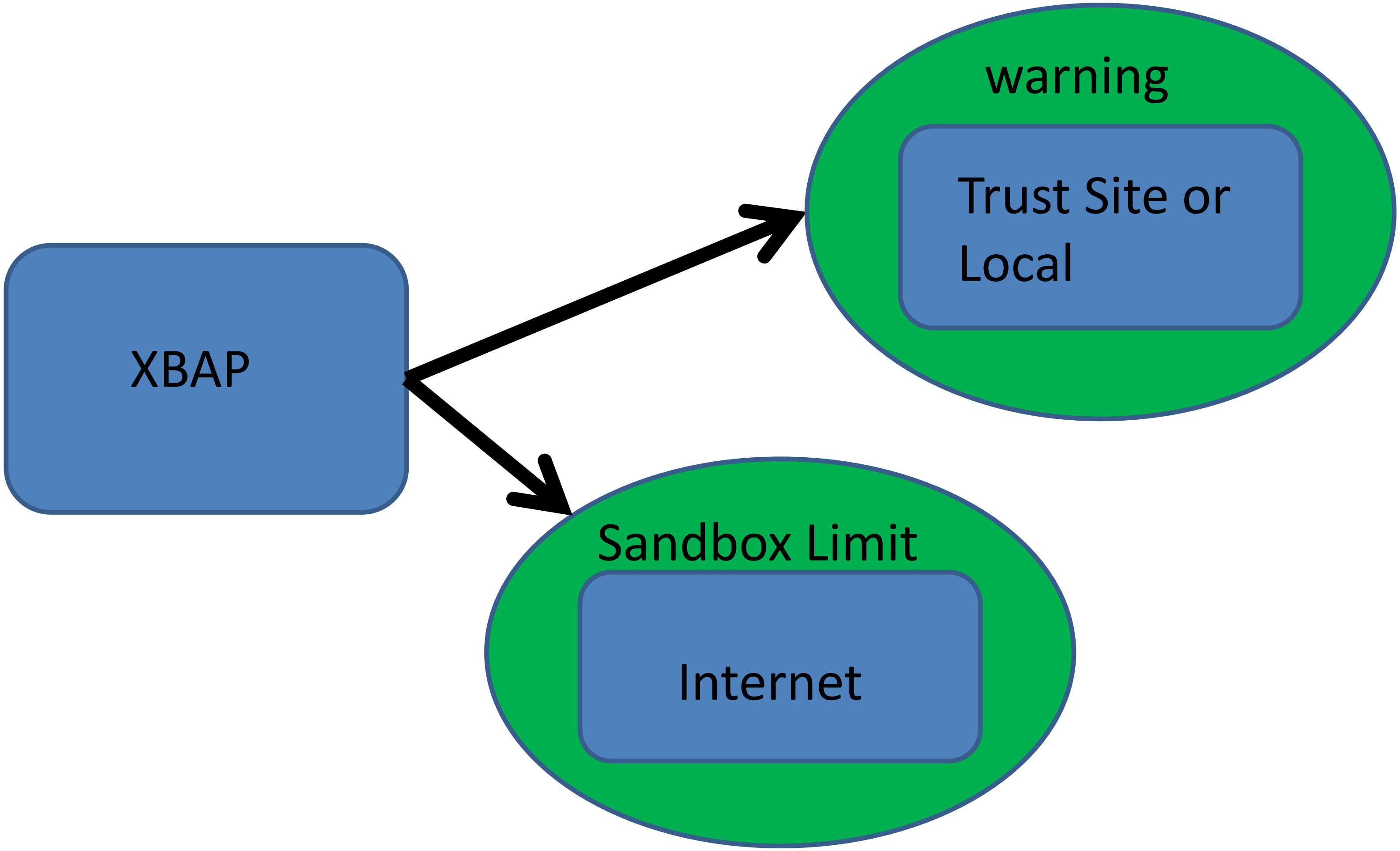
From (Hover over the string below to see the full domain):
C:\Documents and Settings\Administrator\Local Settings\Temp\Rar$EX01.203

Publisher:
Unknown Publisher

While applications can be useful, they can potentially harm your computer. If you do not trust the source, do not run this software. More Information...

Attack	Only .NET no patch	Patched MS11-044	Patched MS12-035
WEB+(ClickOnce full trust)	Must add IE trust site and Warning	Must add IE trust site and Warning	Must add IE trust site and Warning
Local Compress File+(ClickOnce full trust)	No Warning	No Warning	Warning
WEB+(ClickOnce INTERNET)	No Warning	Warning	Warning
Local Compress File+(ClickOnce INTERNET)	No Warning	No Warning	Warning

Design



XBAP

warning

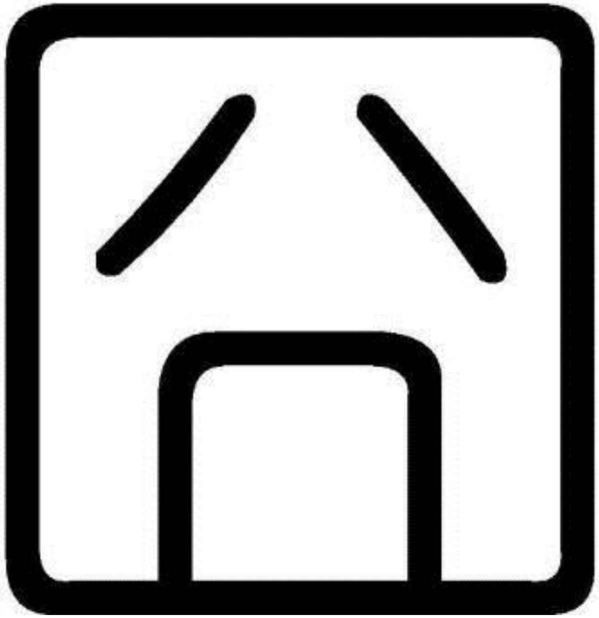
Trust Site or Local

Sandbox Limit

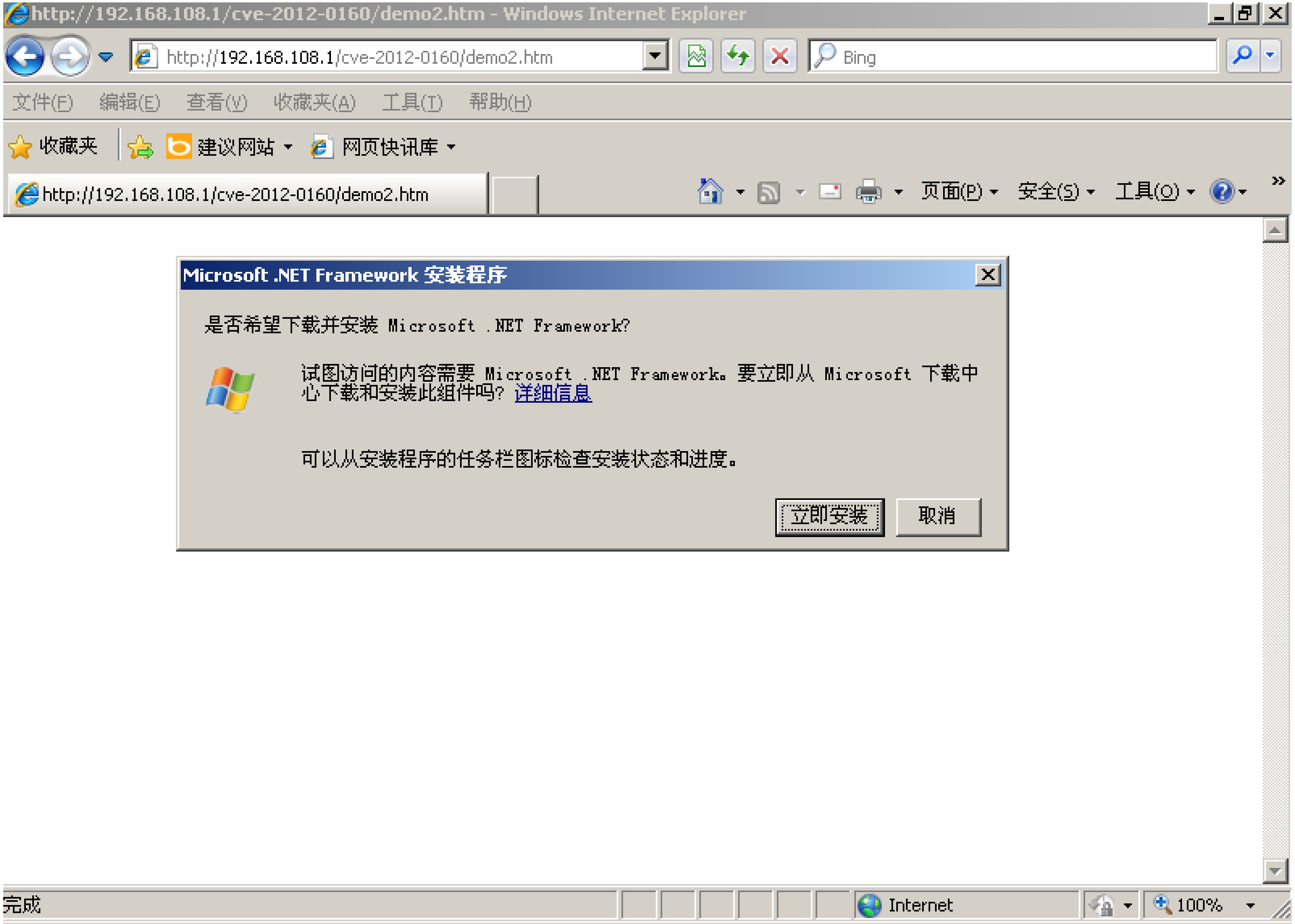
Internet

Any thing Warning!?

- Remember UAC ?
- Any XBAP warning
- Sandbox with warning bypass depend on user’s decide now.



Do you install .Net framework?



http://192.168.108.1/cve-2012-0160/demo2.htm - Windows Internet Explorer
http://192.168.108.1/cve-2012-0160/demo2.htm
Bing
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)
收藏夹
建议网站
网页快讯库
http://192.168.108.1/cve-2012-0160/demo2.htm
页面(P) 安全(S) 工具(O)
完成
Internet
100%

Microsoft .NET Framework 安装程序

是否希望下载并安装 Microsoft .NET Framework?

试图访问的内容需要 Microsoft .NET Framework。要立即从 Microsoft 下载中心下载和安装此组件吗? 详细信息

可以从安装程序的任务栏图标检查安装状态和进度。

立即安装 取消

Summery

- .NET Remote Attack
- .NET Local Attack
- Patched Affect

- TREND always Finds the New Attack TREND

- Thanks