Exploitation of Windows 8 Metro Style Apps

The Subway Line 8

Ming-chieh Pan (Nanika)
Sung-ting Tsai (TT)

black hat USA 2012

About Us

- Security researchers at Trend Micro.
- Doing researches on advanced threats.
- Come out with solutions to solve problems.

Ming-chieh Pan (a.k.a Nanika)

- Staff research engineer of Trend Micro.
- Research on
  - Vulnerability discovery
  - Exploit techniques
  - Malware detection
  - Mobile security
- Windows platform
- Malicious document techniques

- Disclosed
  - CVE-2006-3431 (Excel)
  - CVE-2006-5296 (PowerPoint)
  - And many others (IE, Office, …)
- Talks and Speeches
  - Black Hat USA 2011
  - Syscan Singapore/Taipei/Hong Kong 08/10
  - Hacks in Taiwan Conference 05/06/07/09/10/12

Sung-ting Tsai (a.k.a TT)

- Leader of an advanced threat research team.
- Research topics:
  - New security technology
  - Advanced Persistent Threat
  - Malicious document
  - Malware auto-analyzing system (sandbox technologies)
  - Malware detection
  - System vulnerability and protection
  - Mobile security
- Talks and speeches
  - Black Hat USA 2011
  - Hacks in Taiwan Conference 08’
  - Syscan Singapore 10’

CHROOT Security Group

Windows® 8

TM

TREND MICRO™

black hat USA 2012

- Fancy UI!
- Lots of security improvements!
- Very secure!
- Very robust!

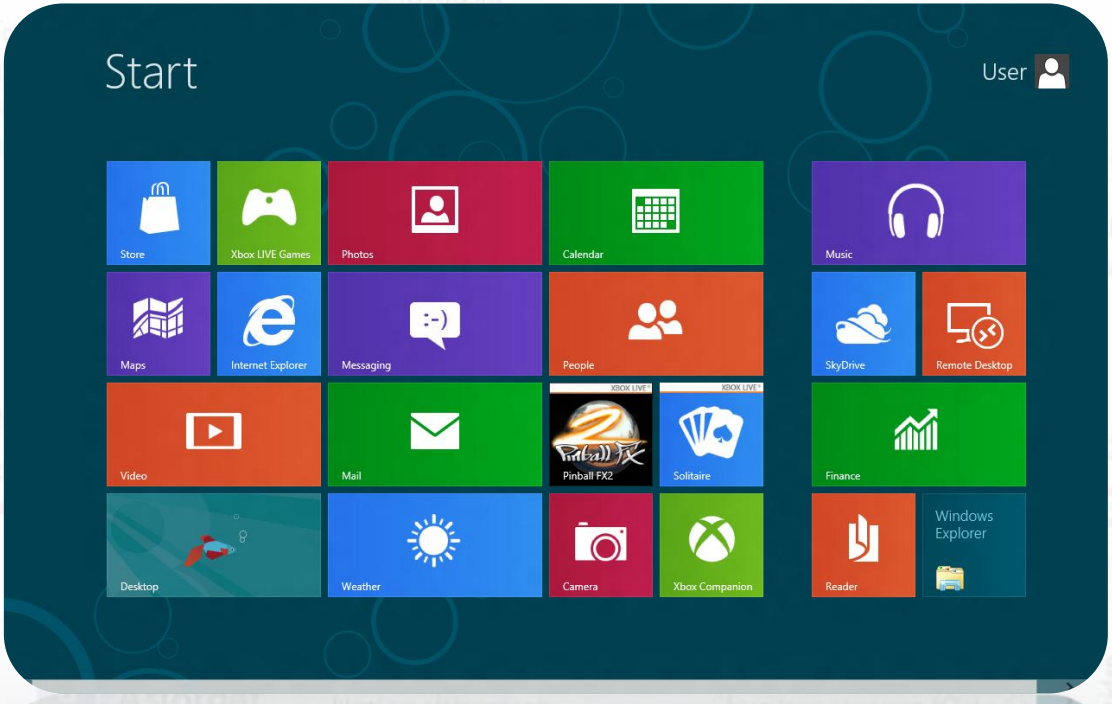
Agenda

- The security design of Metro Style Apps
- Sandbox Bypassing Analysis
- Problems discovery and the attack vectors
  - ALPC / COM / WinRT / Design Logic
- Some issues and responses from MSRC
- Conclusion

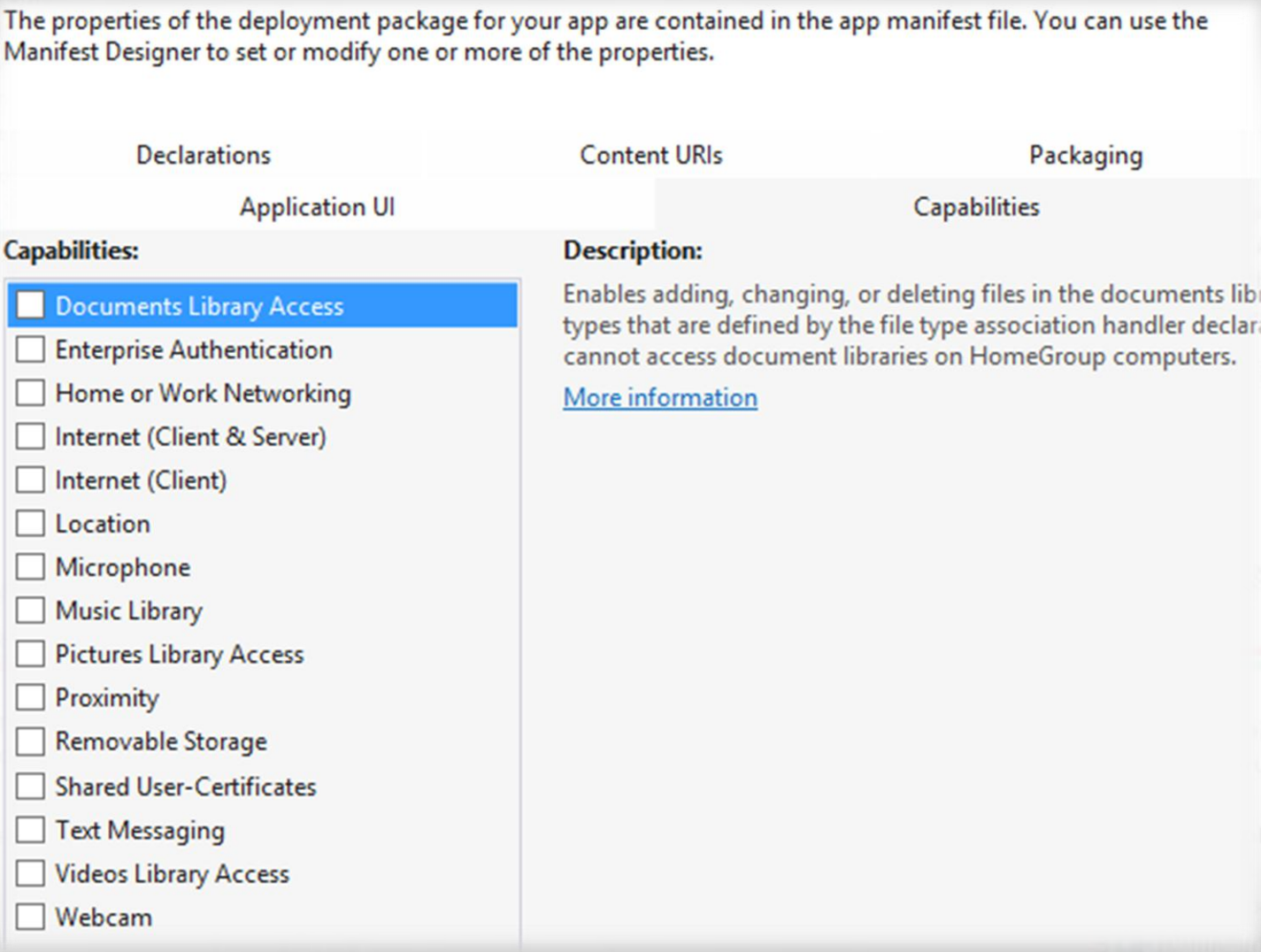
New Security Features in Windows 8

- IE 10
  - EPMIE
  - /GS, /SAFESEH, /DYNAMICBASE,
  - DEP/NX SHEHOP,
  - ASLR
  - HTML5 Sandbox
- New kernel protection
- UEFI
- Application SmartScreen
- Exploit mitigation improvement
- …

WINDOWS 8 AND METRO STYLE APP

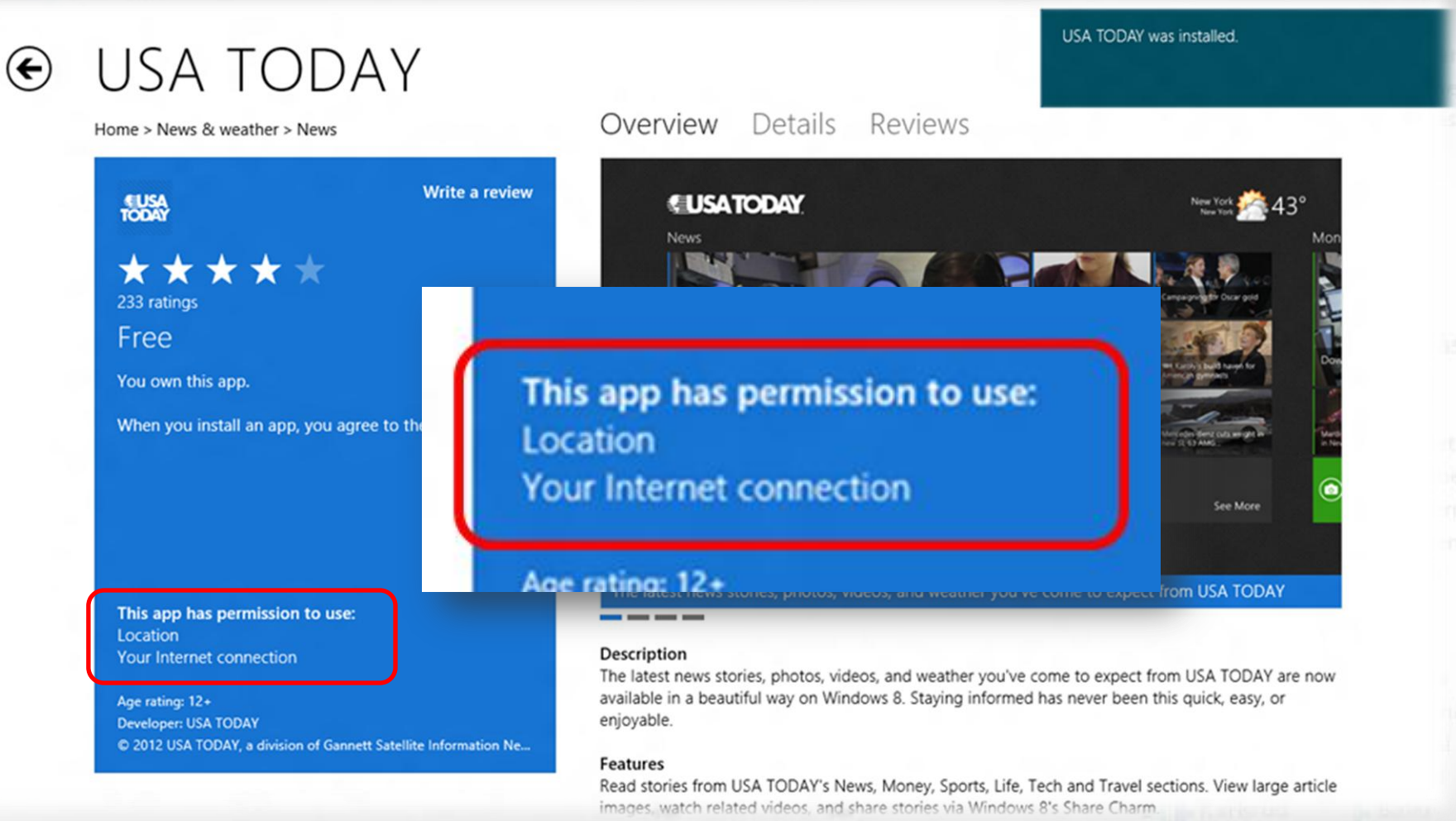


Capability Setting

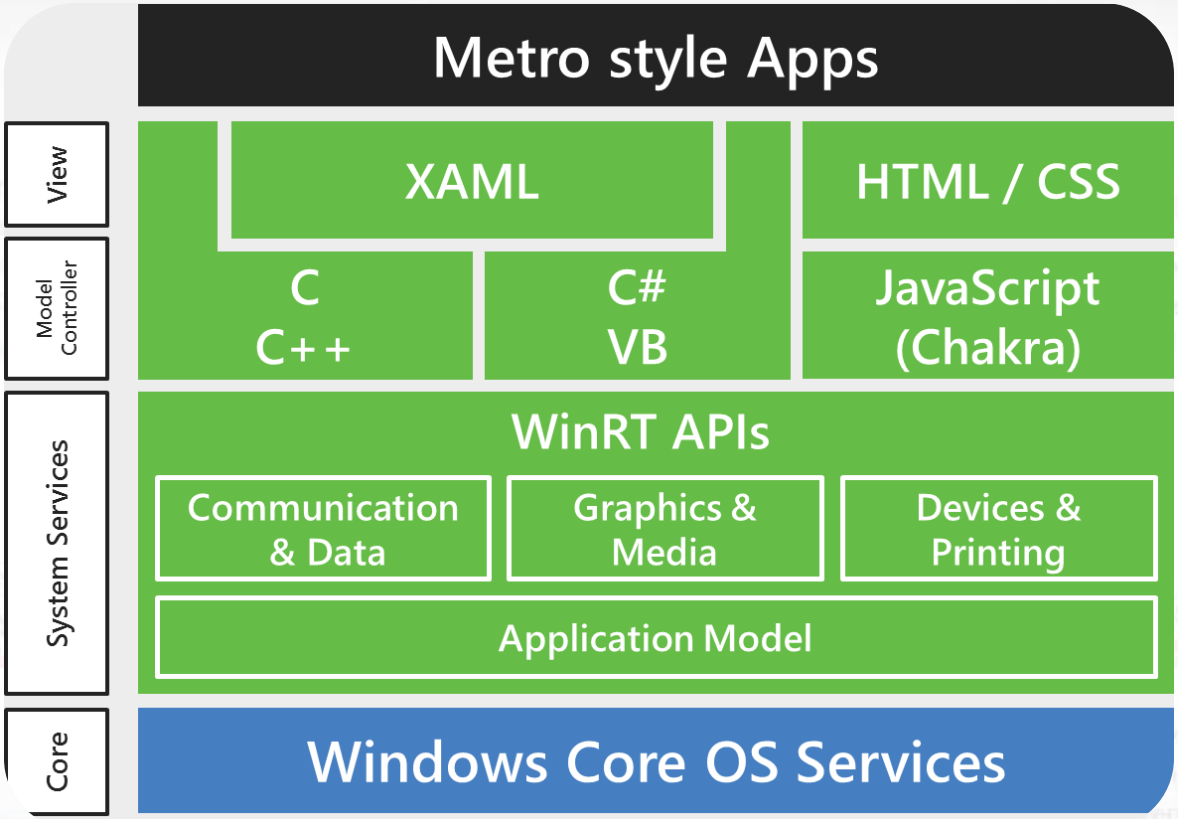


Capabilities

- Network
  - Enterprise auth., client, server & client, Intranet, Text, Messaging, etc.
- File System
  - Documents, Pictures, Music, Video, etc.
- Devices
  - Location (e.g. GPS), Microphone, Proximity (e.g. NFC), Removable storage, etc.
- Things that are specific to an application (local storage, settings, etc.) do not require capabilities.


USA TODAY was installed.
USA TODAY
Home > News & weather > News
Overview
Details
Reviews
Write a review
233 ratings
Free
You own this app.
When you install an app, you agree to th
This app has permission to use:
Location
Your Internet connection
Age rating: 12+
Developer: USA TODAY
© 2012 USA TODAY, a division of Gannett Satellite Information Ne...
USA TODAY
News
New York
43°
See More
This app has permission to use:
Location
Your Internet connection
Age rating: 12+
from USA TODAY
Description
The latest news stories, photos, videos, and weather you've come to expect from USA TODAY are now available in a beautiful way on Windows 8. Staying informed has never been this quick, easy, or enjoyable.
Features
Read stories from USA TODAY's News, Money, Sports, Life, Tech and Travel sections. View large article images, watch related videos, and share stories via Windows 8's Share Charm.

WINRT API

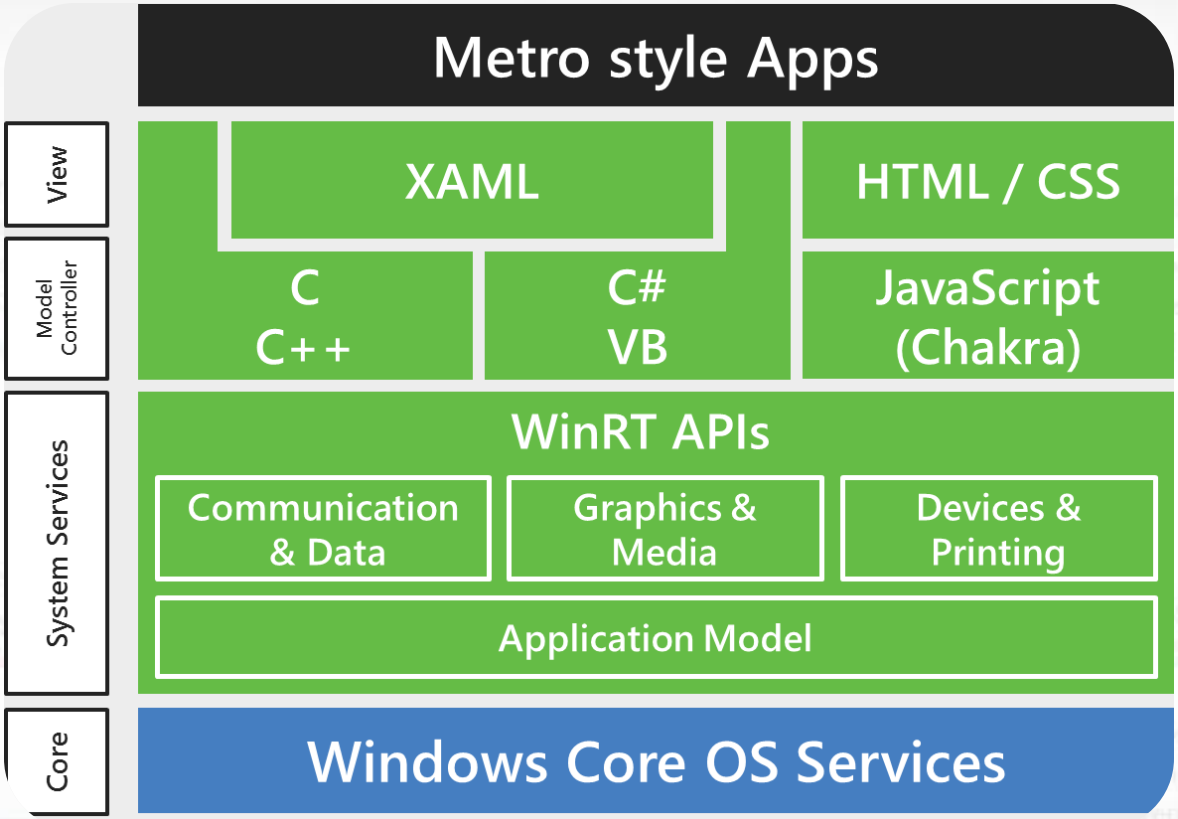


Source: http://blogs.msdn.com/b/b8/archive/2012/02/09/building-windows-for-the-arm-processor-architecture.aspx

WinRT APIs

- Windows Runtime (WinRT API) is the backbone of the new Metro-style apps (also known as Immersive) in the Windows 8 operating system.
- It provides a set of API that can be called from .NET languages (C#, VB.NET, F#), C++, and HTML / JavaScript.
- Apps created for WinRT are
  - Safe
  - Secure
  - Sandboxed

WINRT API

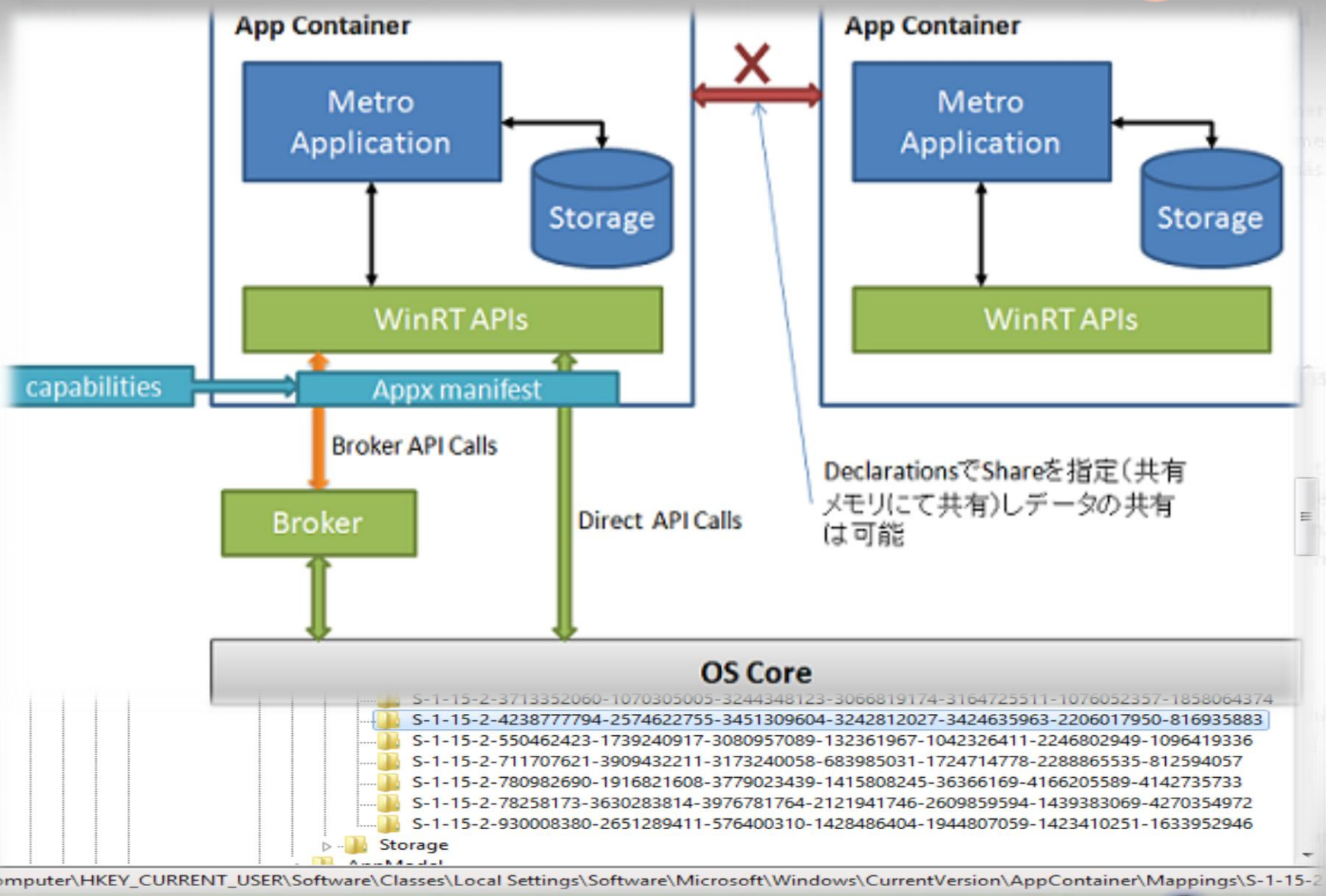

Metro style Apps
View
Model Controller
System Services
Core
XAML
HTML / CSS
C
C++
C#
VB
JavaScript
(Chakra)
WinRT APIs
Communication & Data
Graphics & Media
Devices & Printing
Application Model
Windows Core OS Services

APP CONTAINER

http://www.flickr.com/photos/loufi/3500076/

AppContainer

- What is an application sandbox?
  - A sandbox is a mechanism to isolate untrusted processes.
  - Protecting system from exploit attack.
  - All metro style apps run in AppContainer.
- What does a sandbox contain?
  - Isolated process which runs with very limited rights
  - Broker, a process which could execute specific actions for a isolated process
  - An IPC mechanism to allow isolated processes to communicate with broker



Picture Source: http://ameblo.jp/naoshi1128/entry-11049964906.html

We agree all of these designs really provide a secure execution environment for Metro style apps.

source: http://blogs.msdn.com/b/b8/archive/2012/05/17/delivering-reliable-and-trustworthy-metro-style-apps.aspx

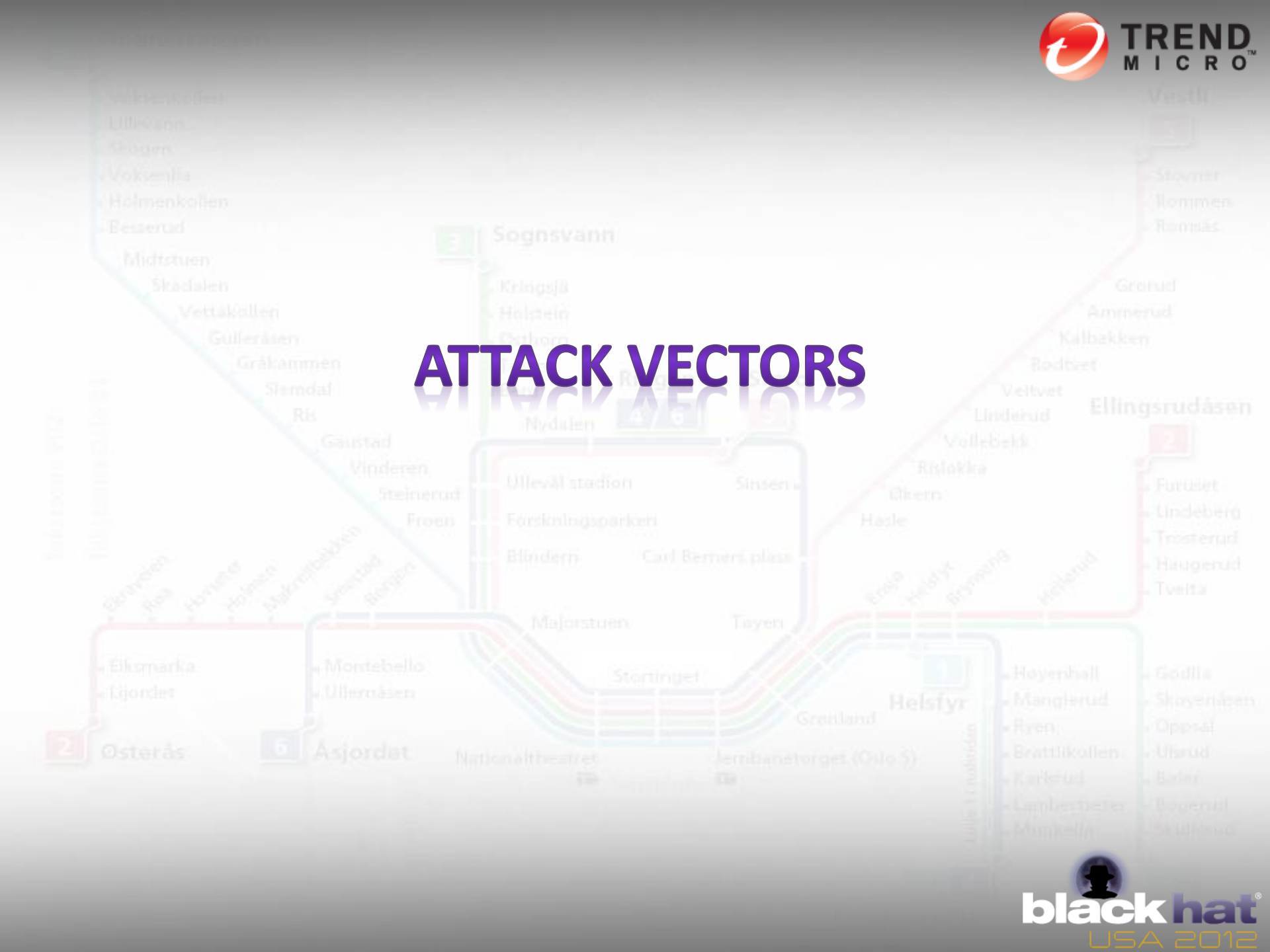
Security design of Metro Style App

- Executed in an "App Container“
  - Secured through a sandbox
  - Severely limited resources access
  - Limited resource access: need explicit permissions
  - Use a restricted subset of .NET and Win32 APIs
- Distributed only through the Windows Store

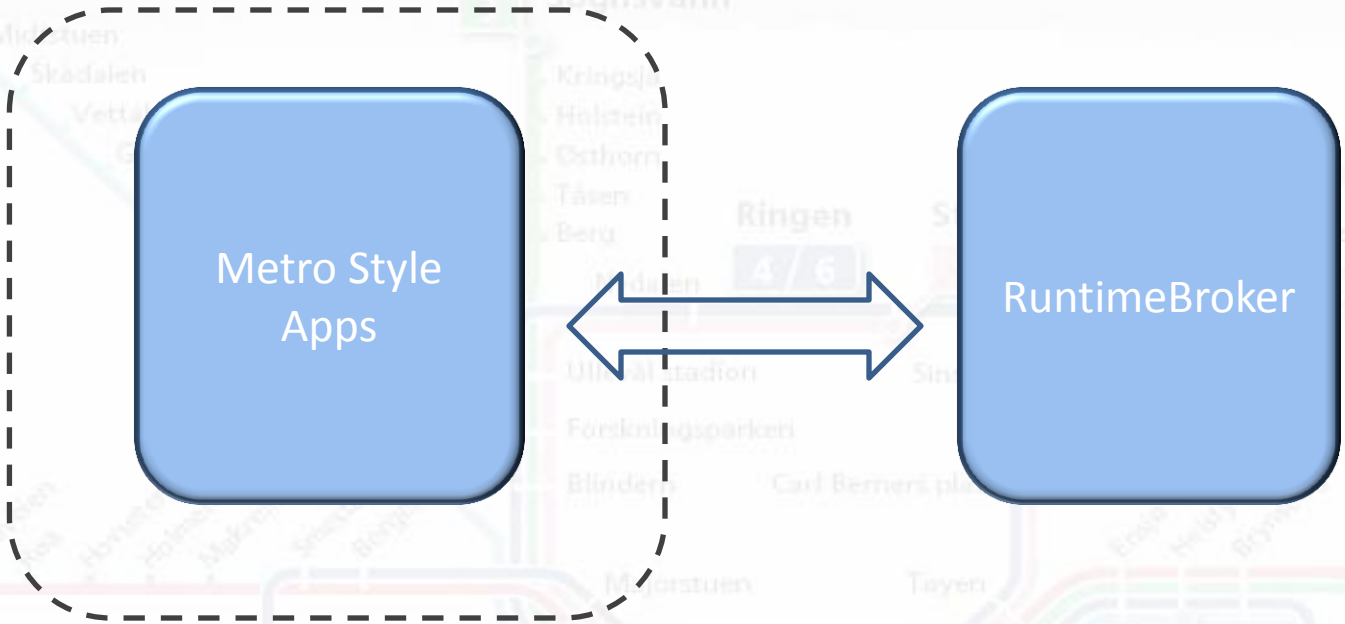
Previous Works on Sandbox Bypassing

- Exploit kernel or privilege escalation vulnerabilities to escape sandbox.
- File system: looking for accessible folders/files and registries, especially some writable locations on the disk. And to see what we can do or what we can get from these places.
- Sending message or keyboard events to outside of sandbox, it might trigger some privilege actions.
- Leverage special handles: some available handles might be used to communicate with other process or resources.

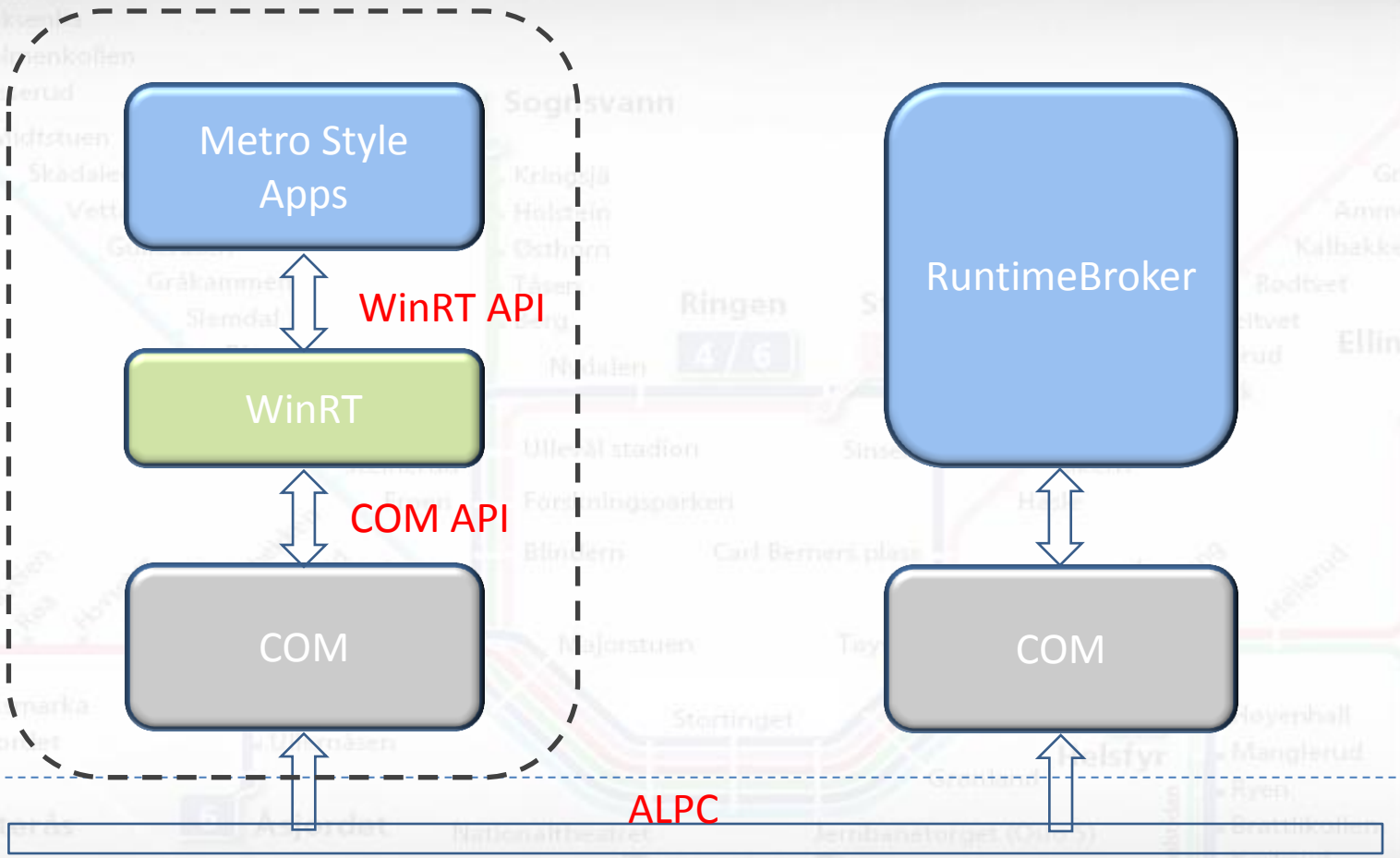
ATTACK VECTORS



Find the Target



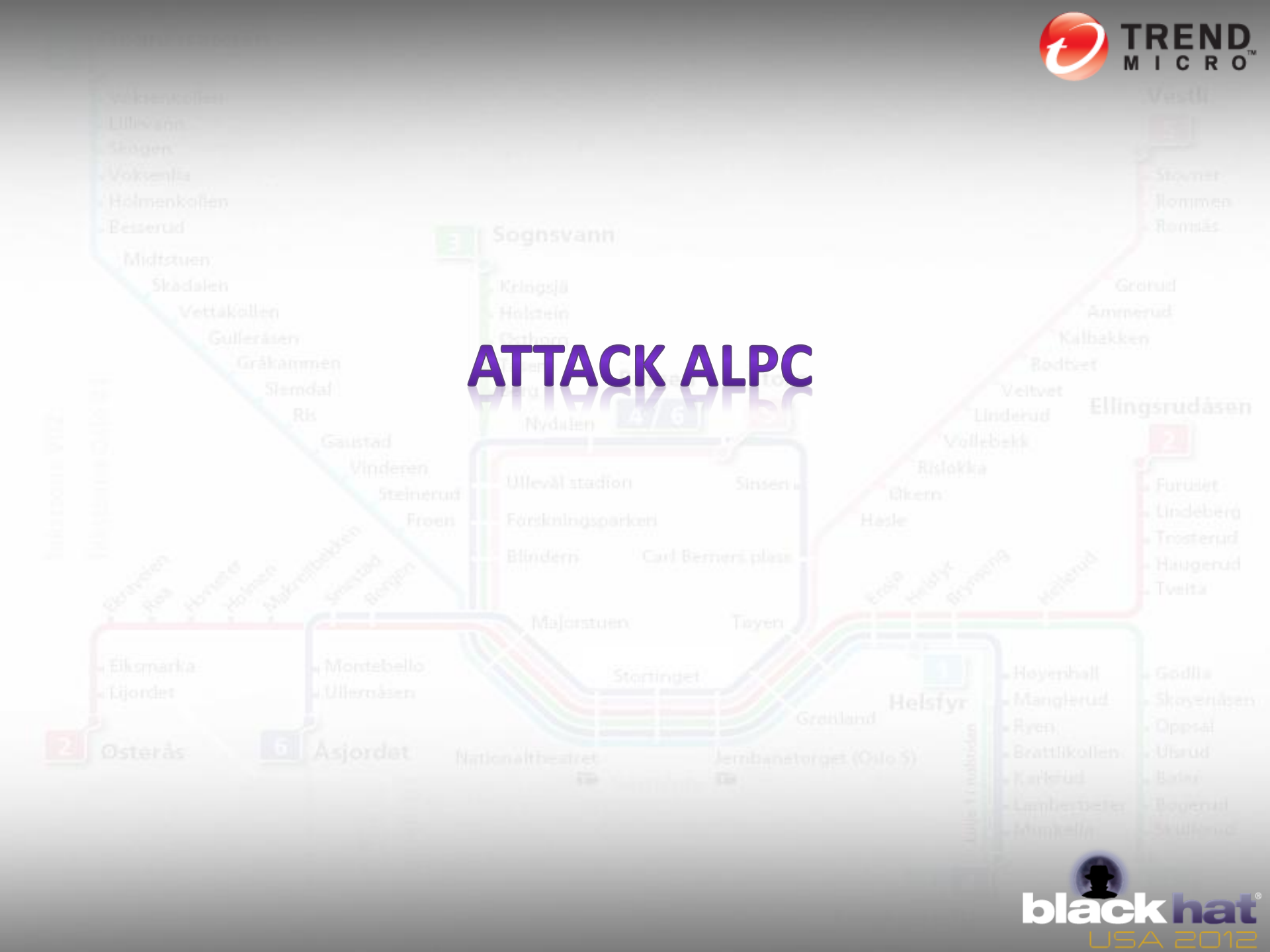
Attack Vectors



AppContainer Sandbox Attack Vectors

- ALPC
- COM
- WinRT
- Design Logic

ATTACK ALPC


Sognsvann
Kringsjå
Holstein
Nydalen
Ullevål stadion
Forskningsparken
Blindern
Carl Berners plass
Majorstuen
Tåyen
Storo
Sinsen
Hasle
Ellingsrudåsen
Furuset
Lindeberg
Trosterud
Haugenud
Tveita
Helsfyr
Grønland
Jernbanetorget (Oslo S)
Nationaltheatret
Stortinget
Montebello
Ullernåsen
Asjordet
Osterås
Eiksmarka
Lijordet
Holmenkollen
Besserud
Midtstuen
Skådalen
Vettakollen
Gulleråsen
Gråkammen
Slemdal
Ris
Gaustad
Vinderen
Steinerud
Frøen
Grorud
Ammerud
Kalbakken
Rødtvet
Veitvet
Linderud
Vollebekk
Ridabakka
Ekern
Romsås
Rommen
Stovner

DEBUG OF ALPC COMMUNICATION

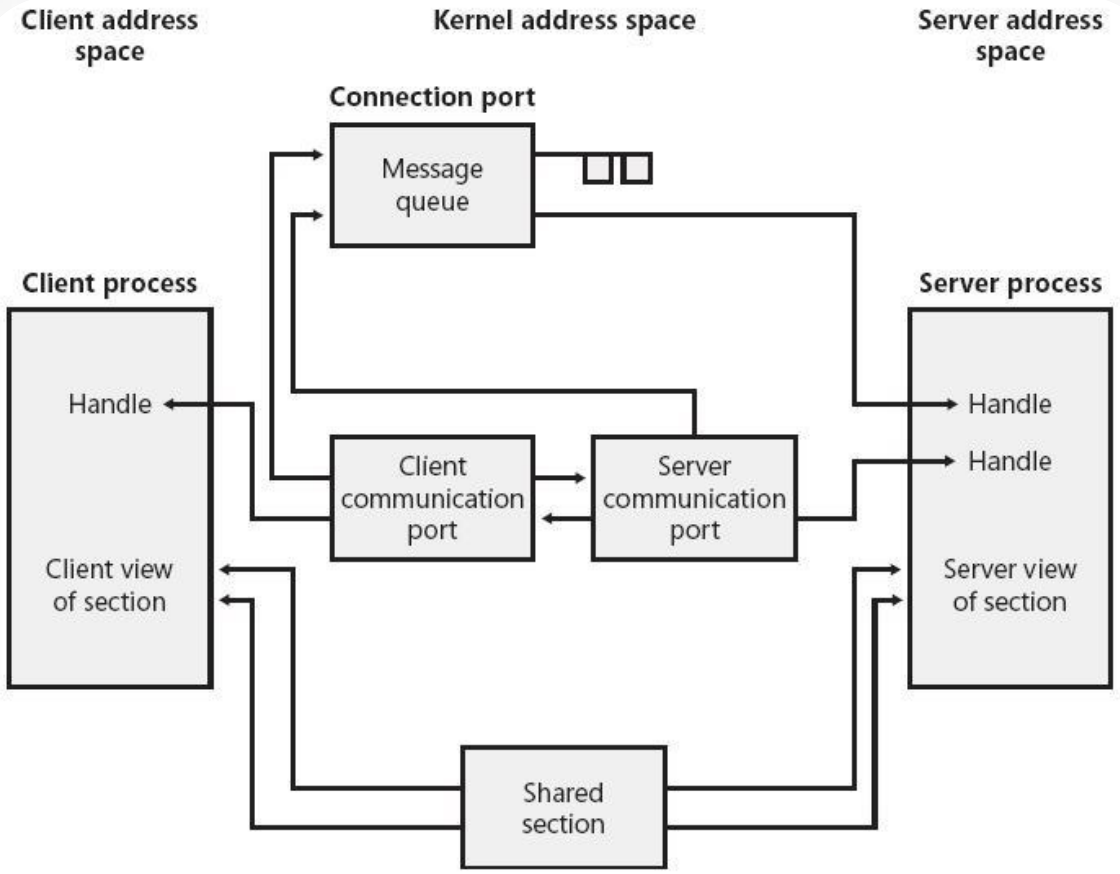
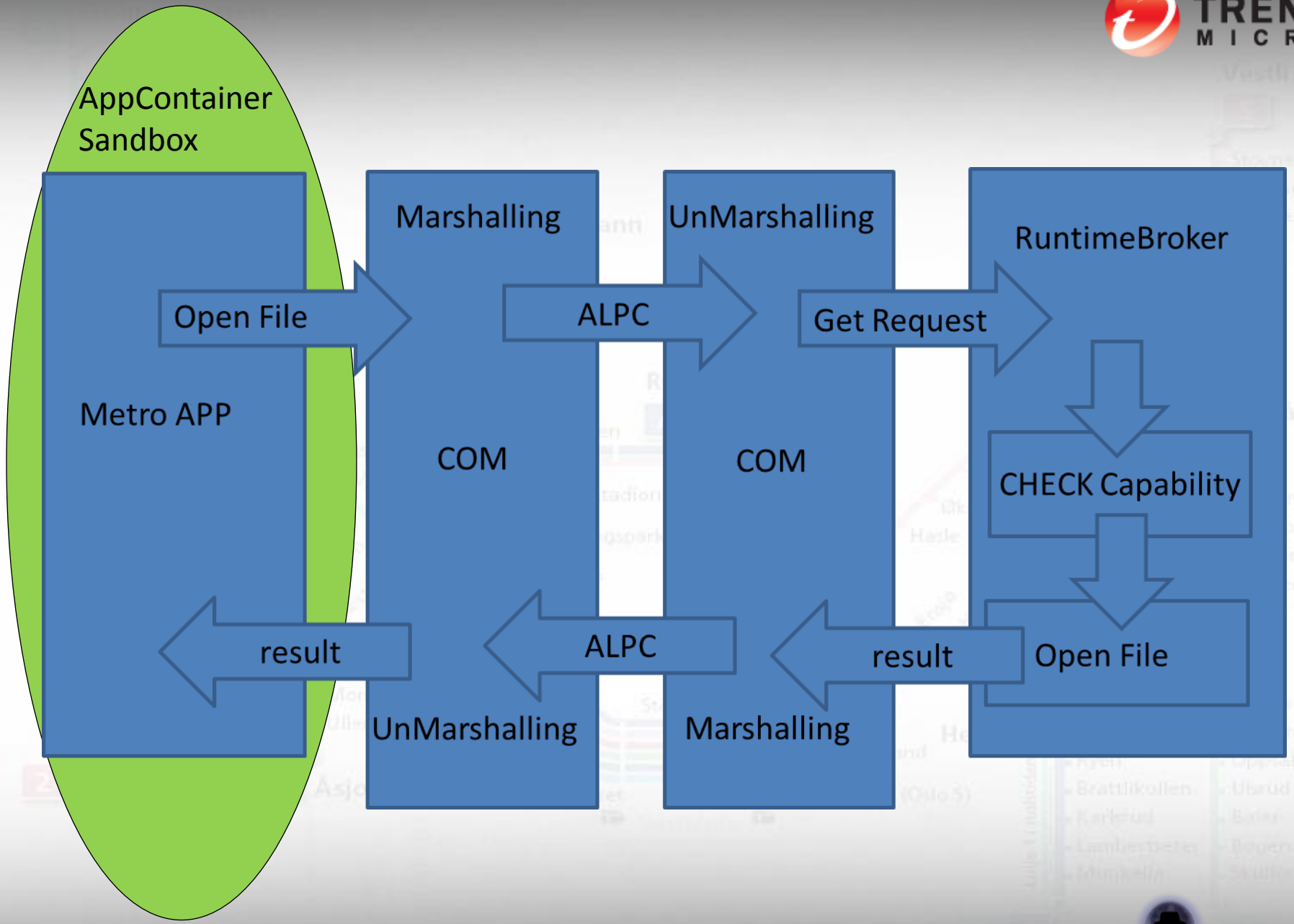


FIGURE 3-27 Use of ALPC ports

Source: http://mba.shengwushibie.com/itbook/BookChapter.asp?id=28217



Ref: http://www.quarkslab.com/dl/2012-HITB-WinRT.pdf

!alpc

0: kd> !alpc /lpp 85c44400

Ports created by the process 85c44400:

Port 856b11b0 is not a connection port.

Ports the process 85c44400 is connected to:

8491b038 0 -> 83ae22e0('ApiPort') 0 852bf6c0('csrss.exe')

83ad9660 0 -> 83ac4540('lsapolicylookup') 0 83aa0300('lsass.exe')

8495b458 0 -> 8571fd98('epmapper') 0 85720c00('svchost.exe')

86058408 0 -> 85722270('actkernel') 0 8570ea00('svchost.exe')

83fc1038 0 -> 857da150('ThemeApiPort') 0 857c0a80('svchost.exe')

8492ee40 0 -> 85ed35b0('OLECE394EC247374B3DB80DFB0D7935') 0 85e4bcc0('explorer.exe')

85f9f2a8 0 -> 83ac43f0('lsasspirpc') 0 83aa0300('lsass.exe')

8513e8f8 0 -> 857bdef8('FontCachePort') 0 857b4c00('svchost.exe')

86000618 0 -> 85d67188('msctf.serverDefault1') 0 85d66700('taskhost.exe')

83abd6f0 0 -> 84967c28('OLE94FA4C860892A252B3E8A6020AC3') 1 84b0f380('RuntimeBroker.')

ALPC syscall

82027f18 823ee774 nt!NtAlpcSetInformation
82027f1c 8247ba70 nt!NtAlpcSendWaitReceivePort
82027f20 824904ce nt!NtAlpcRevokeSecurityContext
82027f24 8248a704 nt!NtAlpcQueryInformationMessage
82027f28 823fdd80 nt!NtAlpcQueryInformation
82027f2c 82408280 nt!NtAlpcOpenSenderThread
82027f30 823fdfdc nt!NtAlpcOpenSenderProcess
82027f34 824916d0 nt!NtAlpcImpersonateClientOfPort
82027f38 824b2f06 nt!NtAlpcDisconnectPort
82027f3c 82490b26 nt!NtAlpcDeleteSecurityContext
82027f40 824cdcd4 nt!NtAlpcDeleteSectionView
82027f44 824dc258 nt!NtAlpcDeleteResourceReserve
82027f48 824cd3e8 nt!NtAlpcDeletePortSection
82027f4c 82490034 nt!NtAlpcCreateSecurityContext
82027f50 824cd72a nt!NtAlpcCreateSectionView
82027f54 824dc024 nt!NtAlpcCreateResourceReserve
82027f58 824ccf96 nt!NtAlpcCreatePortSection
82027f5c 824defc4 nt!NtAlpcCreatePort
82027f60 824e9ae4 nt!NtAlpcConnectPort
82027f64 824e9aa0 nt!NtAlpcConnectPortEx
82027f68 8247bca0 nt!NtAlpcCancelMessage
82027f6c 824f78de nt!NtAlpcAcceptConnectPort

APLC Communication

82027f1c 8247ba70 nt!NtAlpcSendWaitReceivePort

82027f5c 824defc4 nt!NtAlpcCreatePort

82027f60 824e9ae4 nt!NtAlpcConnectPort

82027f6c 824f78de nt!NtAlpcAcceptConnectPort

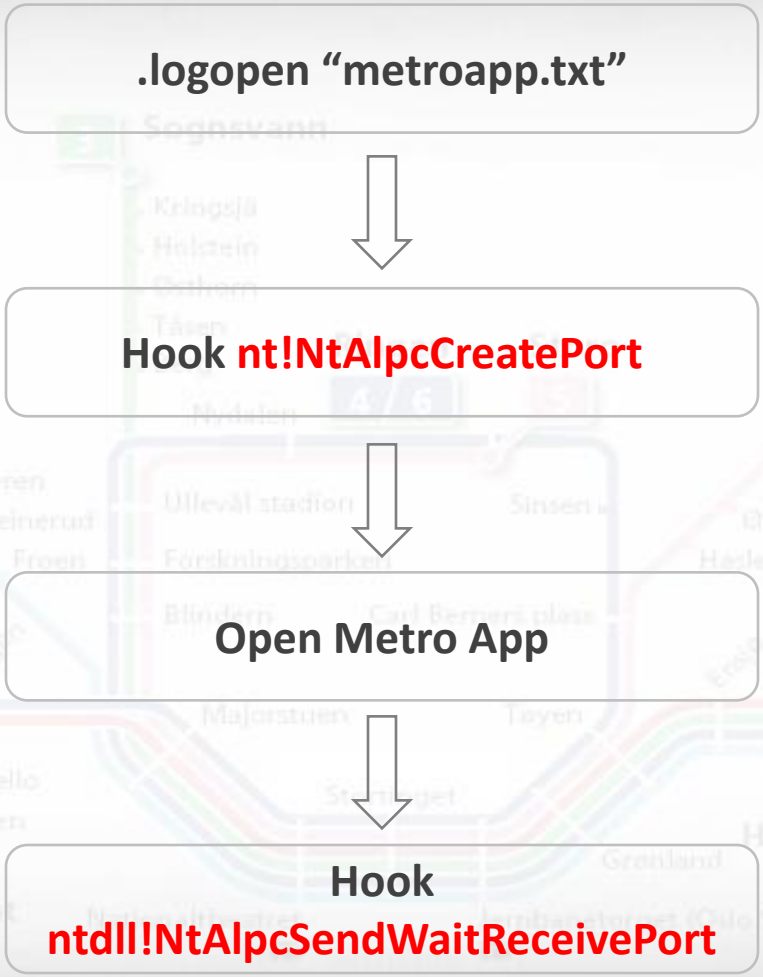
HOOK ALPC communication (1)

```
bp ntdll!NtAlpcSendWaitReceivePort ".catch{r @$t10 =
0xe4c;.if(@$teb != 0){.if(poi(@$teb+20) = @$t10){!handle
poi(esp+0x4);.process; .printf \"PID:%x PortHandle:%x Flags:%x
SendMessage:%x SendMessageAttributes:%x ReceiveMessage:%x
BufferLength:%x ReceiveMessageAttributes:%x
Timeout:%x\r\n\",poi(@$teb+20),poi(esp+0x4),poi(esp+0x8),poi(esp+
0xc),poi(esp+0x10),poi(esp+0x14),poi(esp+0x18),poi(esp+0x1c),poi(esp
+0x20);.if(poi(esp+c)!=0){.printf \"send:\";dt _PORT_MESSAGE
poi(esp+c);db poi(esp+c) l
(poi(poi(esp+c))&0xffff)+0x18;gc;};.if(poi(esp+0x14)!=0){r @$t0 =
poi(esp+0x14);.printf \"recv:\";bp poi(esp) \".process;.if(poi(@$teb+20)
= @$t10){r @$t1 = (poi(@$t0)&0xffff)+0x18;dt _PORT_MESSAGE
@$t0;!alpc /lpp;!alpc /m poi(@$t0+0x10);db @$t0 l @$t1;bc
2;gc;}.else{gc;}\";gc;}}.else {gc;}}.else {gc;}}"
```

HOOK ALPC communication (2)

```
bp nt!NtAlpcCreatePort ".process; .printf \"PID:%x PortHandle:%x ObjectAttributes:%x MaxConnectionInfoLength:%x MaxMessageLength:%x MaxPoolUsage:%x \r\n\",poi(@$teb+20),poi(esp+0x4),poi(esp+0x8),poi(esp+0xc),poi(esp+0x10),poi(esp+0x14);"
bp nt!NtAlpcConnectPort ".process; .printf \"PortHandle:%x PortName:%msu ObjectAttributes:%x PortAttributes:%x Flags:%x RequiredServerSid:%x ConnectionMessage:%x BufferLength:%x OutMessageAttributes:%x InMessageAttributes:%x Timeout:%x \r\n\",poi(esp+0x4),poi(esp+0x8),poi(esp+0xc),poi(esp+0x10),poi(esp+0x14),poi(esp+0x18),poi(esp+0x1c),poi(esp+0x20),poi(esp+0x24),poi(esp+0x28),poi(esp+0x2c) "
bp nt!NtAlpcAcceptConnectPort ".process; .printf \"PortHandle:%x ConnectionPortHandle:%x Flags:%x ObjectAttributes:%x PortAttributes:%x PortContext:%x ConnectionRequest:%x ConnectionMessageAttributes:%x AcceptConnection:%x \r\n\",poi(esp+0x4),poi(esp+0x8),poi(esp+0xc),poi(esp+0x10),poi(esp+0x14),poi(esp+0x18),poi(esp+0x1c),poi(esp+0x20),poi(esp+0x24); “
```

ALPC Analysis Flow



ncalrpc:[\\Sessions\\1\\AppContainerNamedObjects\\S-1-15-2-1115239912-5888679-3094415206-3103815194-10819155-2778485781-2267460753\\RPC Control\\OLE9517A3676FBEC77BBFB0BB30B841]

- {BE0DA0AD-C47E-56DA-BF00-F4344E2FCE93} App.wwa

```
Implicit process is now 85208a00
PID:7ec PortHandle:168 Flags:20000 SendMessage:bfb688 SendMessageAttributes:c0a5cc ReceiveMessage:
   +0x000 u1               : <unnamed-tag>
   +0x004 u2               : <unnamed-tag>
   +0x008 ClientId         : _CLIENT_ID
```

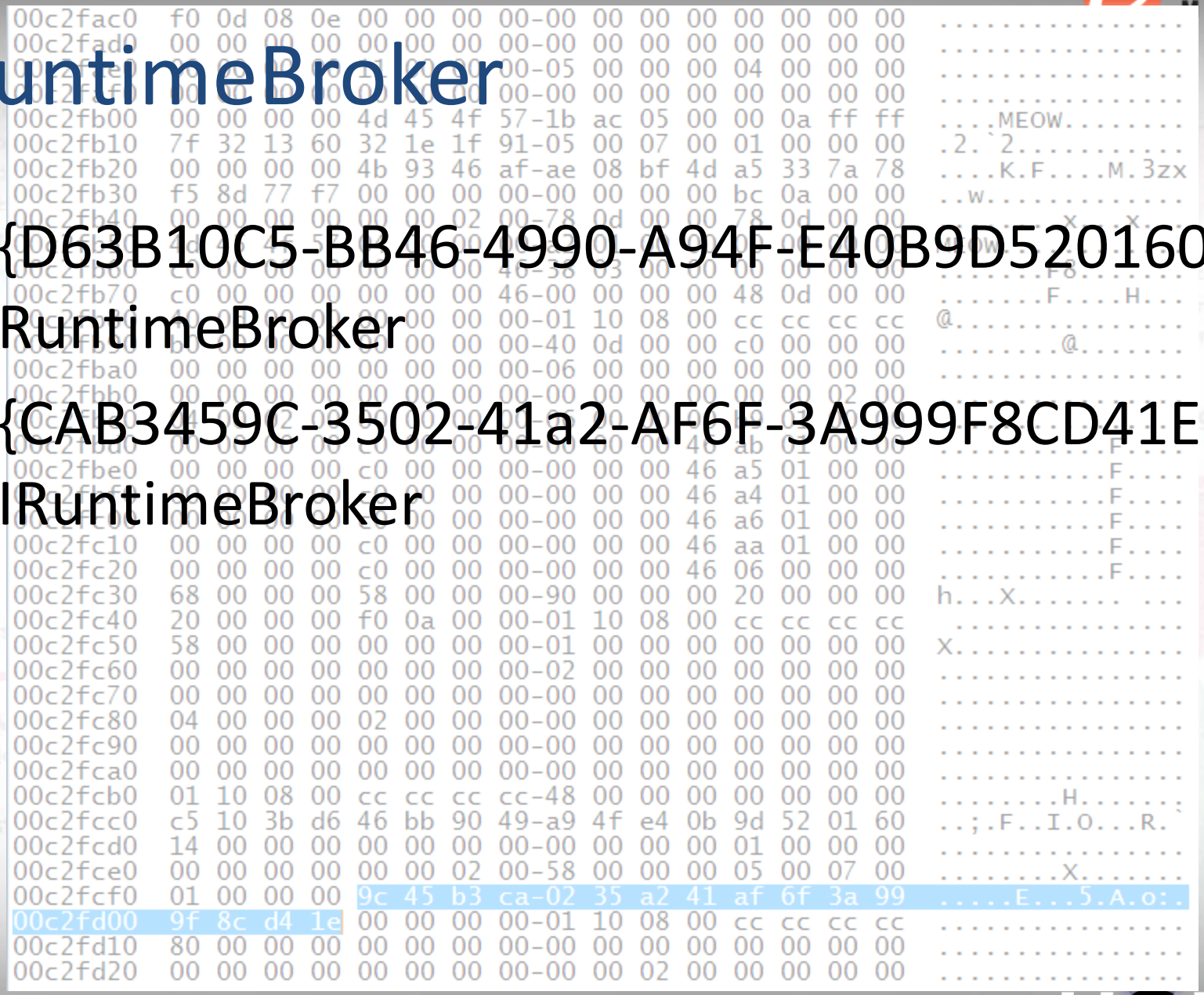
Computer\HKEY_CLASSES_ROOT\ActivatableClasses\CLSID\{BE0DA0AD-C47E-56DA-BF00-F4344E2FCE93}

```
00bfb688  bc 00 d4 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00bfb698  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00bfb6a8  00 00 00 00 0a 00 00 00-03 00 00 00 00 00 00 00  ................
00bfb6b8  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00bfb6c8  00 00 00 00 00 00 00 00-01 00 00 00 37 00 38 00  ............7.8.
00bfb6d8  01 00 00 00 00 00 00 00-00 00 00 00 82 de af 36  ...............6
00bfb6e8  2f 4b ca 42 91 8e 20 d8-07 3b 6b bc 02 00 00 00  /K.B.. ..;k.....
00bfb6f8  02 00 00 00 00 00 00 00-ad a0 0d be 7e c4 da 56  ............~..V
00bfb708  bf 00 f4 34 4e 2f ce 93-d9 68 13 56 a2 61 e6 1f  ...4N/...h.V.a..
00bfb718  03 54 00 00 ec 07 00 00-82 30 64 55 87 38 60 48  .T.......0dU.8`H
00bfb728  02 00 00 c0 00 00 00 00-2d 8a d0 26 36 11 7a 57  ........-..&6.zW
00bfb738  8c b7 8c 3a f0 bf ab 83-d9 68 13 56 a2 61 e6 1f  ...:.....h.V.a..
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActivatableClassId	REG_SZ	App.wwa
PackageMoniker	REG_SZ	c000053d-77bc-4b2f-a138-db89d0eab2bf_1.0.0.1_neutral__4sdae...

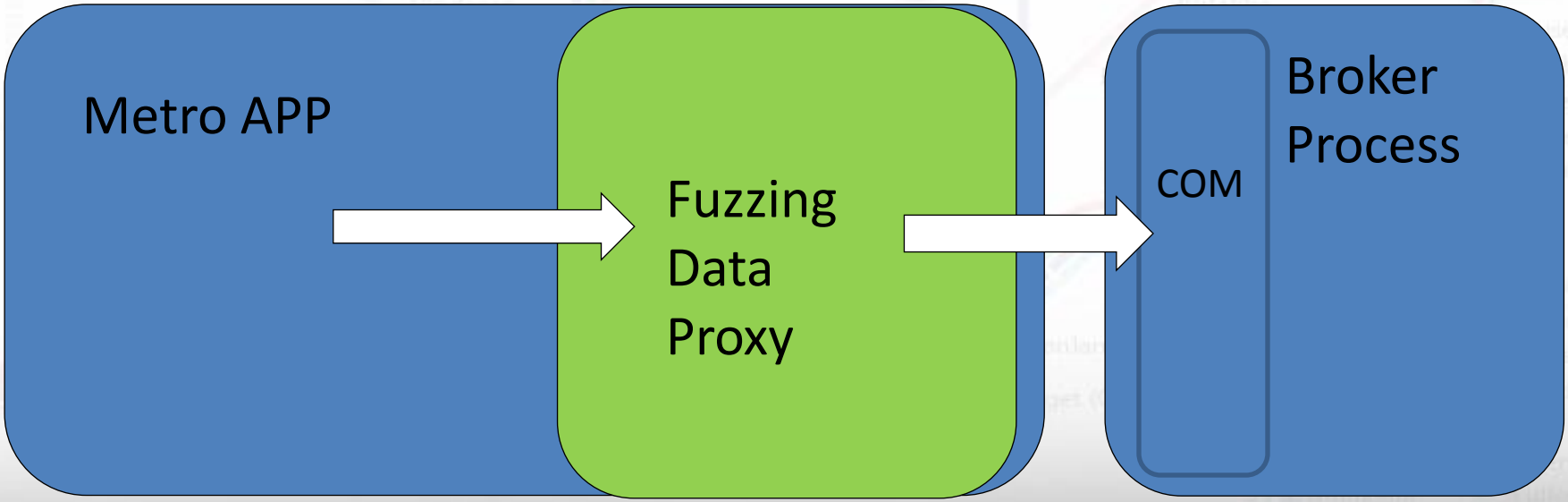
RuntimeBroker

- {D63B10C5-BB46-4990-A94F-E40B9D520160} RuntimeBroker
- {CAB3459C-3502-41a2-AF6F-3A999F8CD41E} IRuntimeBroker

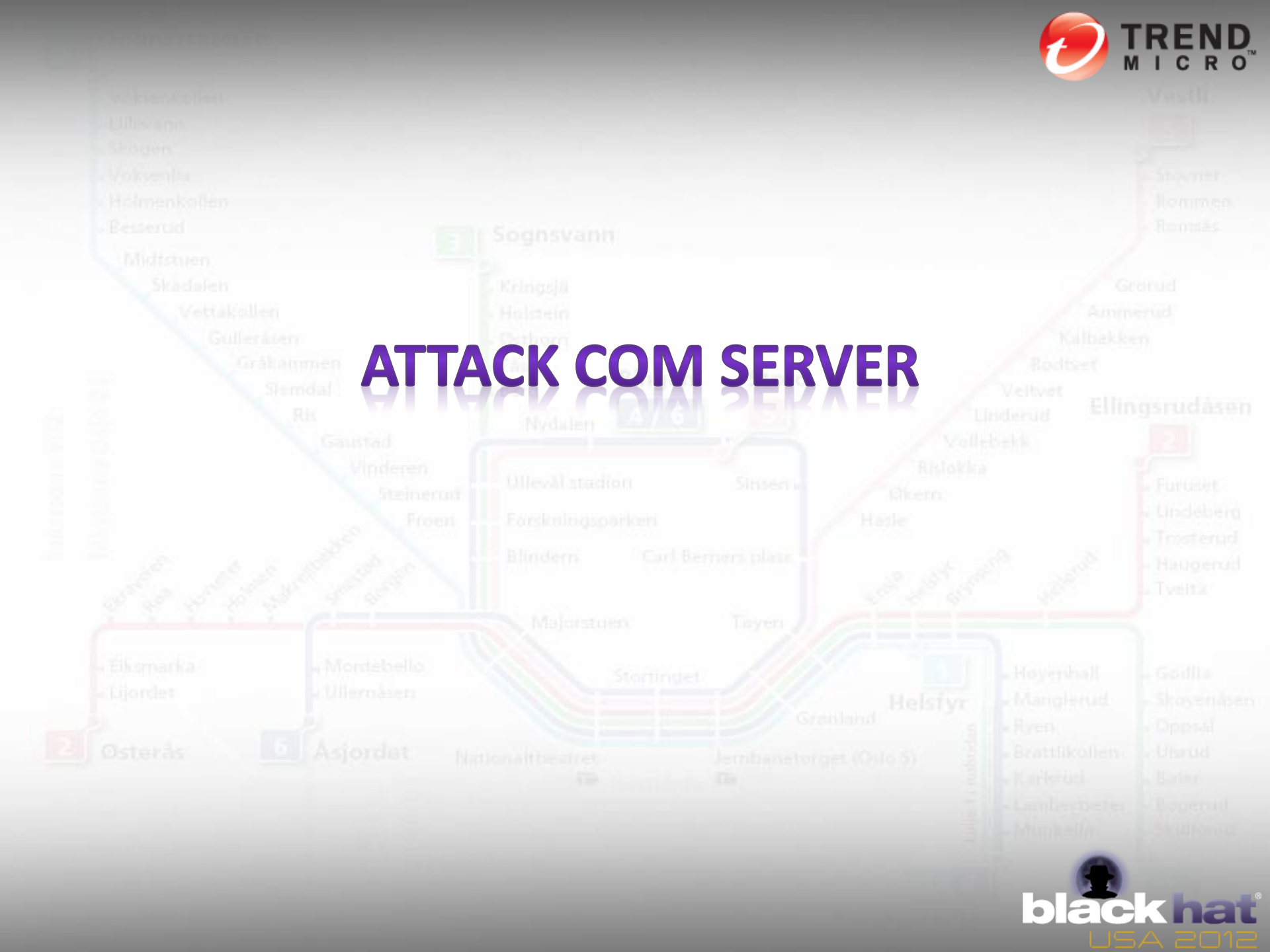


Fuzzing ALPC communication

- Inline ASM
- Hook ntdll!NtAlpcSendWaitReceivePort
- Modify Send Fuzzzing Data



ATTACK COM SERVER



Windows 8 COM

- InInitOrder.blink – kernelbase.dll (instead of kernel32.dll)
- OLE32.dll(Win2000->Win7)
- ComBase.dll (Windows 8)

(nFunctions)	Dword	Word	Dword	szAnsi
000011D	000BB0E0	011C	000EE74D	RoOriginateError

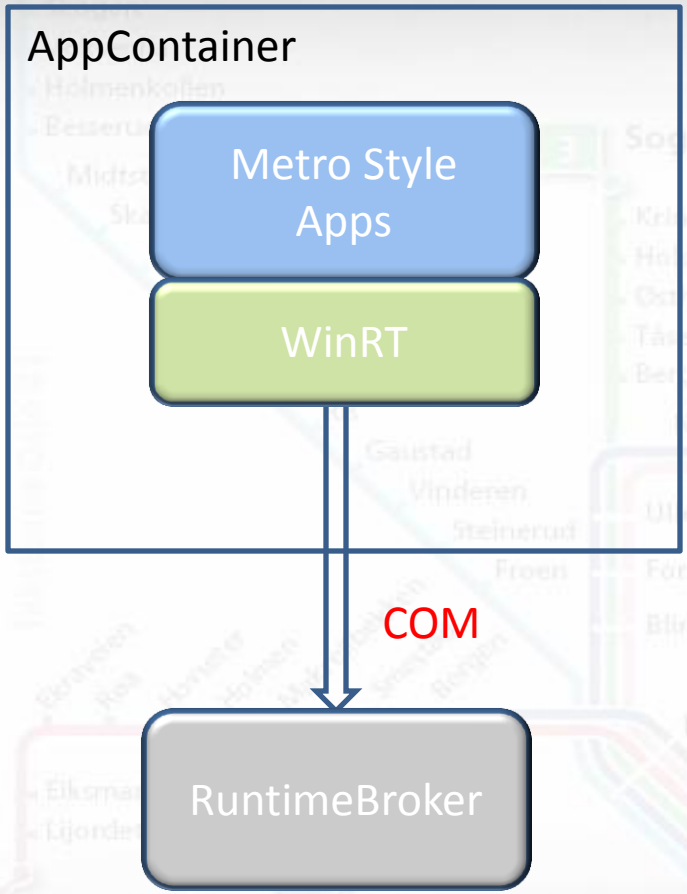
```
0040102D  . 8D45 FC       LEA EAX,DWORD PTR SS:[EBP-4]
00401030  . 50            PUSH EAX
00401031  . 68 F0604000   PUSH com_test.004060F0
00401036  . 6A 04         PUSH 4
00401038  . 6A 00         PUSH 0
0040103A  . 68 C0604000   PUSH com_test.004060C0
0040103F  . FF15 B4604000 CALL DWORD PTR DS:[<&ole32.CoCreateInstance>]   combase.CoCreateInstance
```

0000122	000BB085	0121	000EE7D6	RoReportCapabilityCheckFailure
0000123	000BB7FD	0122	000EE7F5	RoResolveRestrictedErrorInfoReference
0000124	00032F5D	0123	000EE81B	RoRevokeActivationFactories
0000125	000BAC12	0124	000EE837	RoSetErrorReportingFlags
0000126	000BB247	0125	000EE850	RoTransformError
0000127	000BB11D	0126	000EE861	RoTransformErrorW
0000128	00032B9C	0127	000EE873	RoUninitialize
0000129	000331AB	0128	000EE882	RoUnregisterForApartmentShutdown

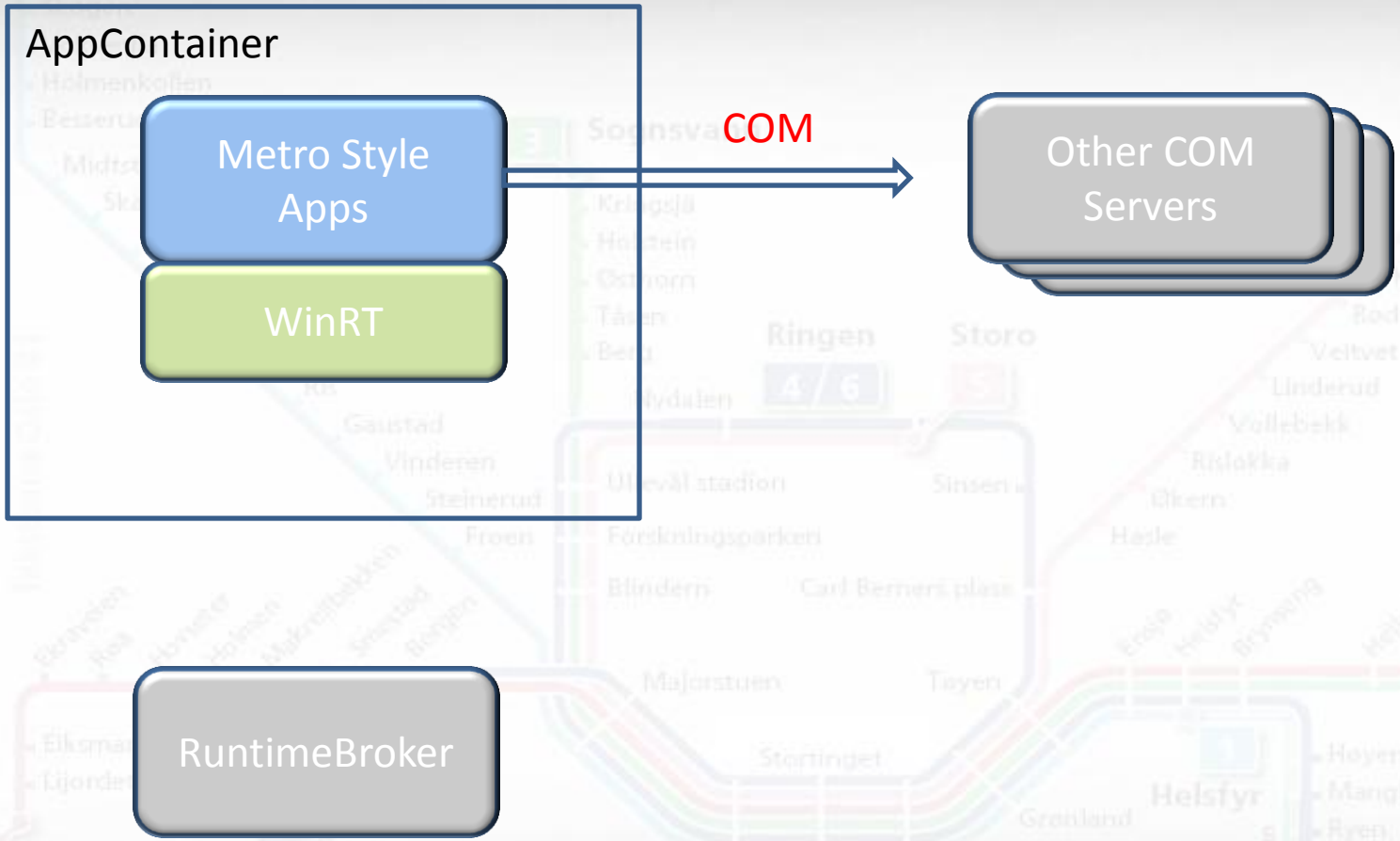
Purpose of COM Testing

- Test stability of COM server
  - Looking for memory problem
- Test functionality of COM server
  - There might be some useful functions can help us to do privileged operations.

The Target - RuntimeBroker



The Target – Other Possibility

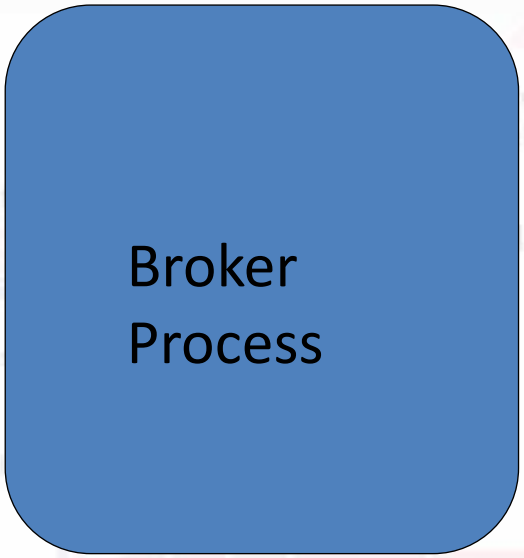


The Target – Privilege

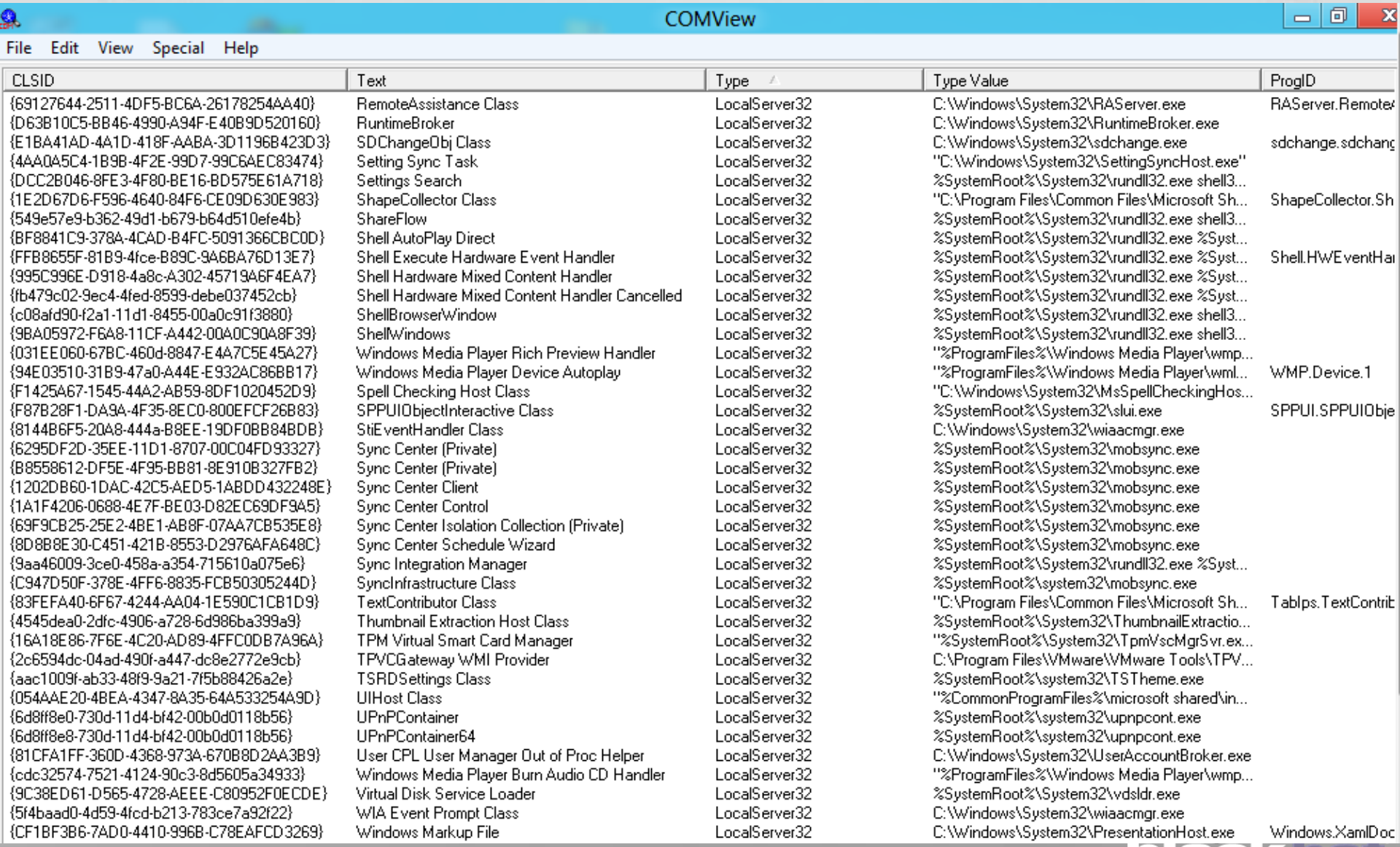
svchost.exe	908	3.39	40,632 K	43,516 K Host Process for Windows S...	Microsoft Corporation	System
dasHost.exe	2880		8,236 K	17,868 K Device Association Framewo...	Microsoft Corporation	System
WUDFHost.exe	3568		1,424 K	4,084 K Windows Driver Foundation -...	Microsoft Corporation	System
TabTip.exe	1140	0.74	8,268 K	23,520 K Touch Keyboard and Handw...	Microsoft Corporation	High

Examples:

- Metro APP COM interface
- RuntimeBroker.exe ->Medium
- ImeBroker.exe ->Medium
- Wkspbroker.exe->Medium
- Tabtip.exe -> High
- …



The Target – Available COM



CLSID	Text	Type	Type Value	ProgID
{69127644-2511-4DF5-BC6A-26178254AA40}	RemoteAssistance Class	LocalServer32	C:\Windows\System32\RAServer.exe	RAServer.Remote
{D63B10C5-BB46-4990-A94F-E40B9D520160}	RuntimeBroker	LocalServer32	C:\Windows\System32\RuntimeBroker.exe	
{E1BA41AD-4A1D-418F-AABA-3D1196B423D3}	SDChangeObj Class	LocalServer32	C:\Windows\System32\sdchange.exe	sdchange.sdchang
{4AA0A5C4-1B9B-4F2E-99D7-99C6AEC83474}	Setting Sync Task	LocalServer32	"C:\Windows\System32\SettingSyncHost.exe"	
{DCC2B046-8FE3-4F80-BE16-BD575E61A718}	Settings Search	LocalServer32	%SystemRoot%\System32\rundll32.exe shell3...	
{1E2D67D6-F596-4640-84F6-CE09D630E983}	ShapeCollector Class	LocalServer32	"C:\Program Files\Common Files\Microsoft Sh...	ShapeCollector.Sh
{549e57e9-b362-49d1-b679-b64d510efe4b}	ShareFlow	LocalServer32	%SystemRoot%\System32\rundll32.exe shell3...	
{BF8841C9-378A-4CAD-B4FC-5091366CBC0D}	Shell AutoPlay Direct	LocalServer32	%SystemRoot%\System32\rundll32.exe %Syst...	
{FFB8655F-81B9-4fce-B89C-9A6BA76D13E7}	Shell Execute Hardware Event Handler	LocalServer32	%SystemRoot%\System32\rundll32.exe %Syst...	Shell.HWEventHa
{995C996E-D918-4a8c-A302-45719A6F4EA7}	Shell Hardware Mixed Content Handler	LocalServer32	%SystemRoot%\System32\rundll32.exe %Syst...	
{fb479c02-9ec4-4fed-8599-debe037452cb}	Shell Hardware Mixed Content Handler Cancelled	LocalServer32	%SystemRoot%\System32\rundll32.exe %Syst...	
{c08afd90-f2a1-11d1-8455-00a0c91f3880}	ShellBrowserWindow	LocalServer32	%SystemRoot%\System32\rundll32.exe shell3...	
{9BA05972-F6A8-11CF-A442-00A0C90A8F39}	ShellWindows	LocalServer32	%SystemRoot%\System32\rundll32.exe shell3...	
{031EE060-67BC-460d-8847-E4A7C5E45A27}	Windows Media Player Rich Preview Handler	LocalServer32	"%ProgramFiles%\Windows Media Player\wmp...	
{94E03510-31B9-47a0-A44E-E932AC86BB17}	Windows Media Player Device Autoplay	LocalServer32	"%ProgramFiles%\Windows Media Player\wml...	WMP.Device.1
{F1425A67-1545-44A2-AB59-8DF1020452D9}	Spell Checking Host Class	LocalServer32	"C:\Windows\System32\MsSpellCheckingHos...	
{F87B28F1-DA9A-4F35-8EC0-800EFCF26B83}	SPPUIObjectInteractive Class	LocalServer32	%SystemRoot%\System32\slui.exe	SPPUI.SPPUIObje
{8144B6F5-20A8-444a-B8EE-19DF0BB84BDB}	StiEventHandler Class	LocalServer32	C:\Windows\System32\wiaacmgr.exe	
{6295DF2D-35EE-11D1-8707-00C04FD93327}	Sync Center (Private)	LocalServer32	%SystemRoot%\System32\mobsync.exe	
{B8558612-DF5E-4F95-BB81-8E910B327FB2}	Sync Center (Private)	LocalServer32	%SystemRoot%\System32\mobsync.exe	
{1202DB60-1DAC-42C5-AED5-1ABDD432248E}	Sync Center Client	LocalServer32	%SystemRoot%\System32\mobsync.exe	
{1A1F4206-0688-4E7F-BE03-D82EC69DF9A5}	Sync Center Control	LocalServer32	%SystemRoot%\System32\mobsync.exe	
{69F9CB25-25E2-4BE1-AB8F-07AA7CB535E8}	Sync Center Isolation Collection (Private)	LocalServer32	%SystemRoot%\System32\mobsync.exe	
{8D8B8E30-C451-421B-8553-D2976AFA648C}	Sync Center Schedule Wizard	LocalServer32	%SystemRoot%\System32\mobsync.exe	
{9aa46009-3ce0-458a-a354-715610a075e6}	Sync Integration Manager	LocalServer32	%SystemRoot%\System32\rundll32.exe %Syst...	
{C947D50F-378E-4FF6-8835-FCB50305244D}	SyncInfrastructure Class	LocalServer32	%SystemRoot%\system32\mobsync.exe	
{83FEFA40-6F67-4244-AA04-1E590C1CB1D9}	TextContributor Class	LocalServer32	"C:\Program Files\Common Files\Microsoft Sh...	TabIps.TextContrib
{4545dea0-2dfc-4906-a728-6d986ba399a9}	Thumbnail Extraction Host Class	LocalServer32	%SystemRoot%\System32\ThumbnailExtractio...	
{16A18E86-7F6E-4C20-AD89-4FFC0DB7A96A}	TPM Virtual Smart Card Manager	LocalServer32	"%SystemRoot%\System32\TpmVscMgrSvr.ex...	
{2c6594dc-04ad-490f-a447-dc8e2772e9cb}	TPVCGateway WMI Provider	LocalServer32	C:\Program Files\VMware\VMware Tools\TPV...	
{aac1009f-ab33-48f9-9a21-7f5b88426a2e}	TSRDSettings Class	LocalServer32	%SystemRoot%\system32\TSTheme.exe	
{054AAE20-4BEA-4347-8A35-64A533254A9D}	UIHost Class	LocalServer32	"%CommonProgramFiles%\microsoft shared\in...	
{6d8ff8e0-730d-11d4-bf42-00b0d0118b56}	UPnPContainer	LocalServer32	%SystemRoot%\system32\upnpcont.exe	
{6d8ff8e8-730d-11d4-bf42-00b0d0118b56}	UPnPContainer64	LocalServer32	%SystemRoot%\system32\upnpcont.exe	
{81CFA1FF-360D-4368-973A-670B8D2AA3B9}	User CPL User Manager Out of Proc Helper	LocalServer32	C:\Windows\System32\UserAccountBroker.exe	
{cdc32574-7521-4124-90c3-8d5605a34933}	Windows Media Player Burn Audio CD Handler	LocalServer32	"%ProgramFiles%\Windows Media Player\wmp...	
{9C38ED61-D565-4728-AEEE-C80952F0ECDE}	Virtual Disk Service Loader	LocalServer32	%SystemRoot%\System32\vdsldr.exe	
{5f4baad0-4d59-4fcd-b213-783ce7a92f22}	WIA Event Prompt Class	LocalServer32	C:\Windows\System32\wiaacmgr.exe	
{CF1BF3B6-7AD0-4410-996B-C78EAFCD3269}	Windows Markup File	LocalServer32	C:\Windows\System32\PresentationHost.exe	Windows.XamlDoc

Looking for Local Servers

svchost.exe	632		2,600 K	6,896 K Host Process for Windows S...	Microsoft Corporation	System
dllhost.exe	3556		1,388 K	3,852 K COM Surrogate	Microsoft Corporation	System
RuntimeBroker.exe	3368		960 K	3,340 K Runtime Broker	Microsoft Corporation	Medium
CredentialUIBroker.exe	2428		1,136 K	3,860 K Credential Manager UI Host	Microsoft Corporation	Medium
svchost.exe	908	3.39	40,632 K	43,516 K Host Process for Windows S...	Microsoft Corporation	System
dasHost.exe	2880		8,236 K	17,868 K Device Association Framewo...	Microsoft Corporation	System
WUDFHost.exe	3568		1,424 K	4,084 K Windows Driver Foundation -...	Microsoft Corporation	System
TabTip.exe	1140	0.74	8,268 K	23,520 K Touch Keyboard and Handw...	Microsoft Corporation	High

No icon Available

{de50c7bb-faa7-4a7f-ba47-bf0efcfe433d} <no name>

{DE50C7BB-FAA7-4A7F-BA47-BF0EFCFE433D}

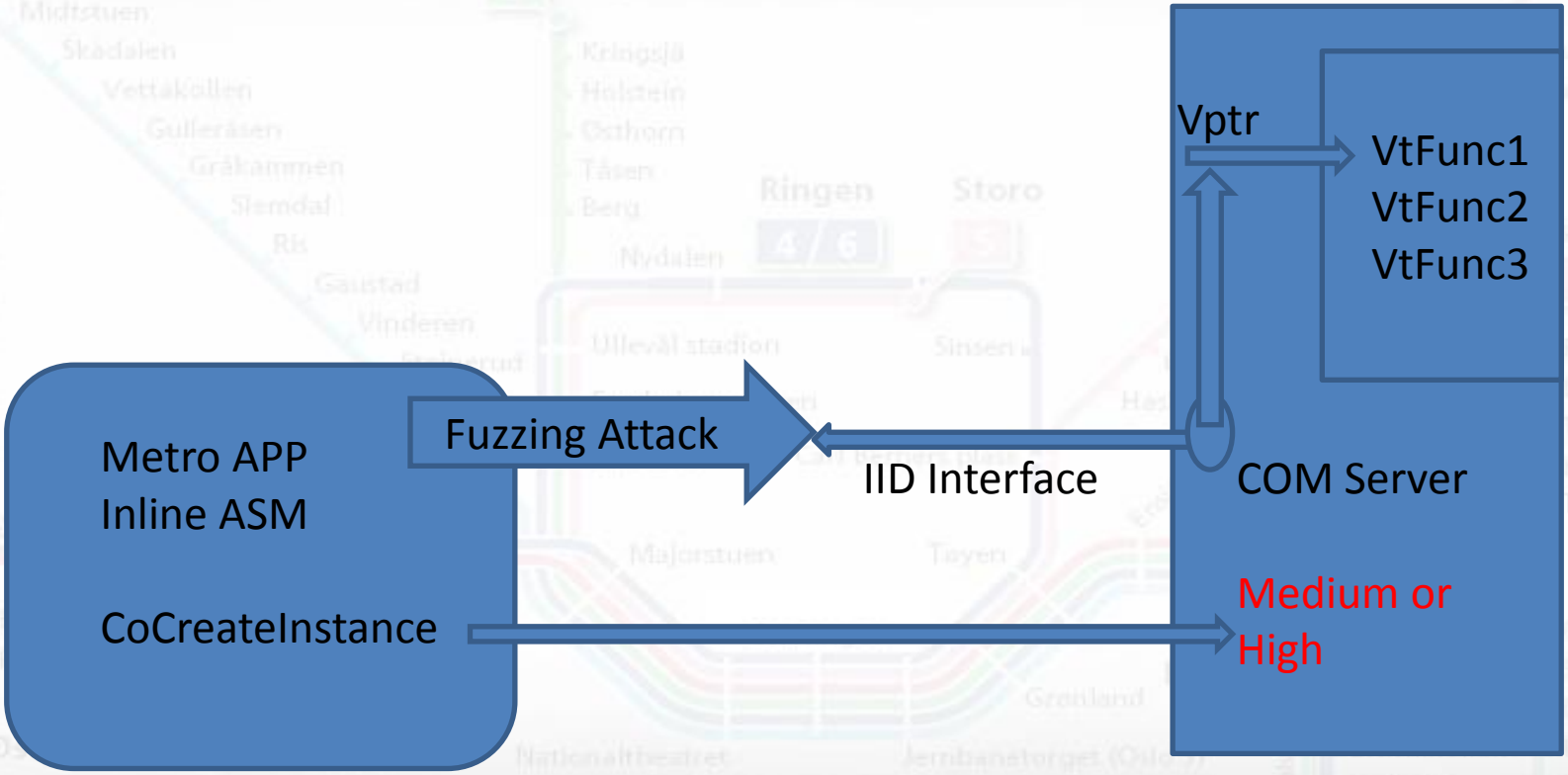
Registry | Implementation | Activation | Launch Permissions | Access Permissions

○ Use default launch permissions

◉ Use these launch permissions:

User/Group	Can Launch
APPLICATION PACKAGE AUTHORITY\ALL APPLICA...	Yes
NT AUTHORITY\SELF	Yes

Attack COM server in Metro App



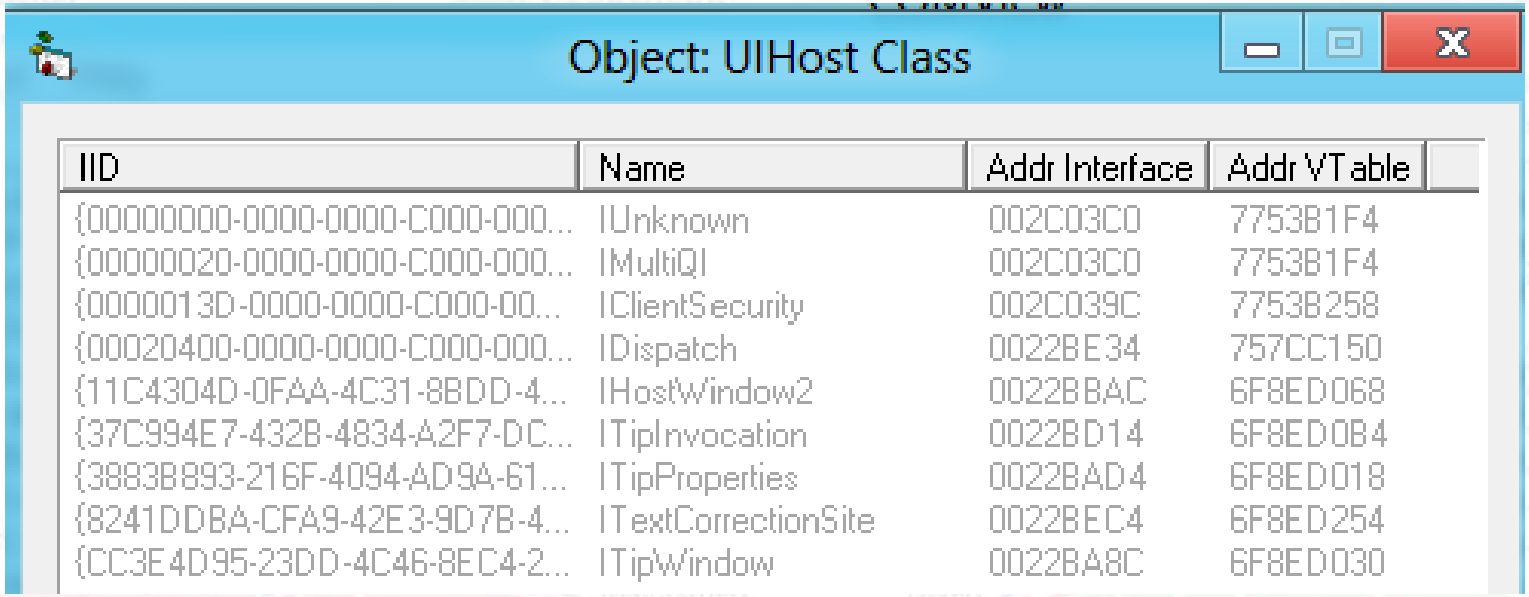
CLSIDs of imebroker

- {69B1A7D7-C09E-40E9-A1DF-688007A2D9E4} //imebroker.exe
- {9A4B1918-0A2F-4422-89DD-35B3F455999C} //imebroker.exe
- {A4FBCBC6-4BE5-4C3D-8AB5-8B873357A23E} //imebroker.exe
- {BA6EE7D8-190D-423A-93CC-1270E6599195} //imebroker.exe
- {C658E5BD-817B-41C8-8FB6-5B2B386A40EA} //imebroker.exe
- {DE50C7BB-FAA7-4A7F-BA47-BF0EFCFE433D} //imebroker.exe
- {DF46CD07-4F86-42F0-8FA9-35C3CE55D77B} //imebroker.exe

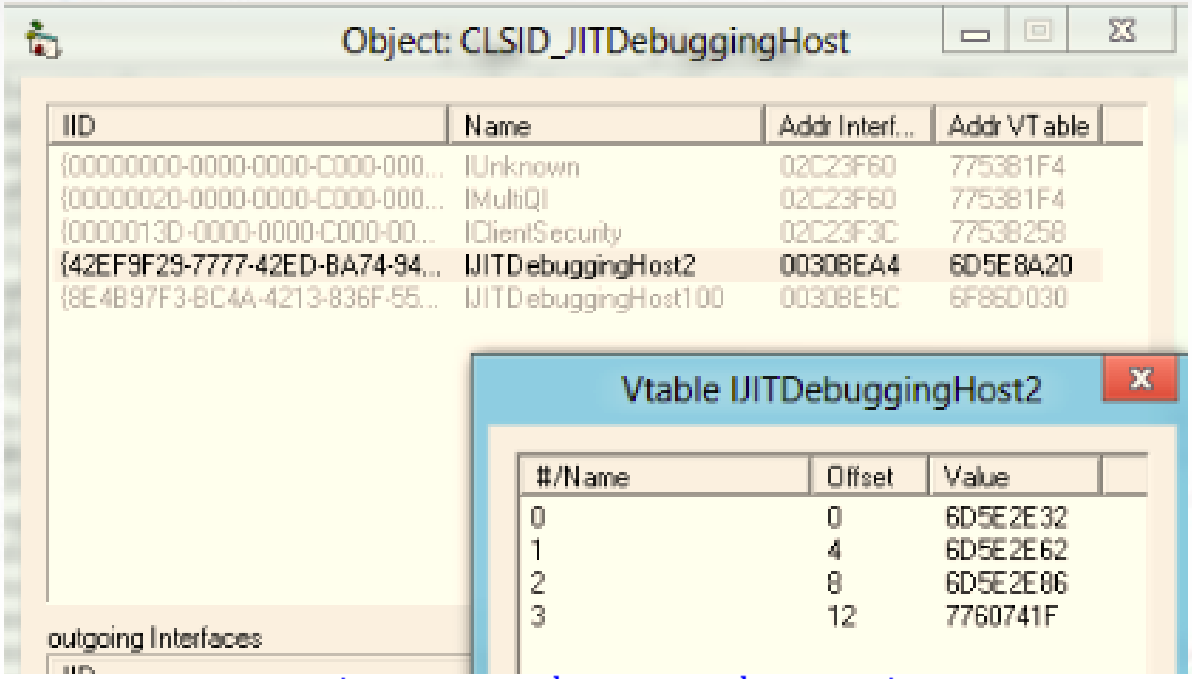
Clsid with “ALL APPLICATION PACKAGE” launch permission

- {7FC12E96-4CB7-4ABD-ADAA-EF7845B10629}//CredentialUIBroker.exe
- {31337EC7-5767-11CF-BEAB-00AA006C3606}//AuthHost.exe
- {36BBB745-0999-4FD8-A538-4D4D84E4BD09}//CLSID_JITDebuggingHost
- {228826AF-02E1-4226-A9E0-99A855E455A6}//Immersive Shell Broker unknow
- {A47979D2-C419-11D9-A5B4-001185AD2B89}//Network List Manager unknow
- {C4D6E899-E38A-4838-9188-0B98EE3175E6}//ProgrammabilityManager Class unknow
- {D63B10C5-BB46-4990-A94F-E40B9D520160}//RuntimeBroker.exe
- {549E57E9-B362-49D1-B679-B64D510EFE4B}//ShareFlow
- {7B6EA1D5-03C2-4AE4-B21C-8D0515CC91B7}//Shell Create Object Task Server unknow
- {F1425A67-1545-44A2-AB59-8DF1020452D9}//Spell Checking Host Class
- {D6E88812-F325-4DC1-BBC7-23076618E58D}//TsfManager Class unknow TabTip.exe
- {6B19643A-0CD7-4563-B710-BDC191FCAD3B}//TSFstateManager Class unknow TabTip.exe
- {054AAE20-4BEA-4347-8A35-64A533254A9D}//high UIHost Class TabTip.exe
- {4CE576FA-83DC-4F88-951C-9D0782B4E376}//UIHostNoLaunch Class unknow TabTip.exe
- {2F93C02D-77F9-46B4-95FB-8CBB81EEB62C}//DevicesFlow
- {19C65143-6230-42FA-A58E-7D9FA9BE2EB5}//WorkspaceBroker Class wkspbroker.exe

Looking for Interfaces of Local Server

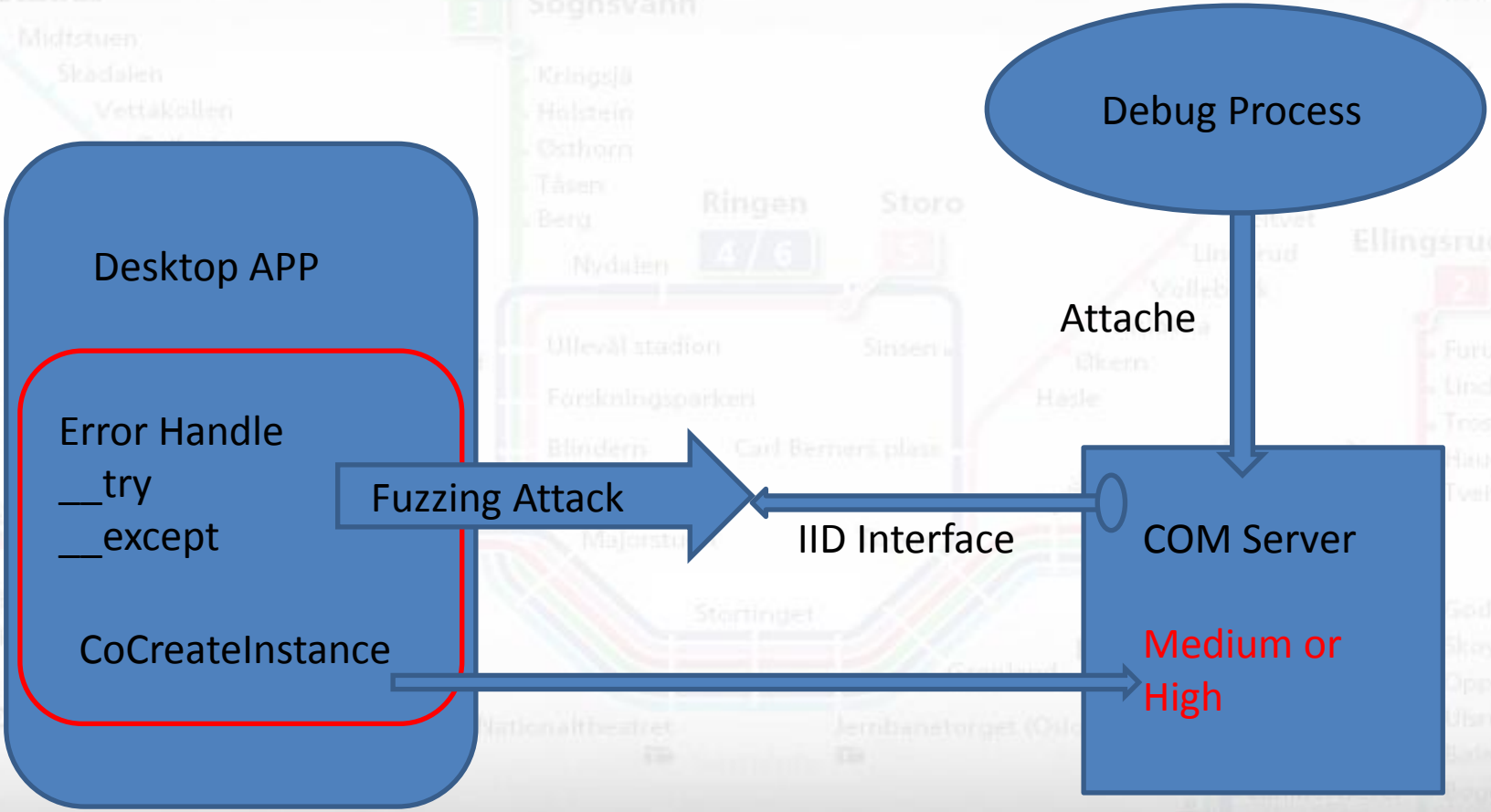


Looking for functions of Local Server

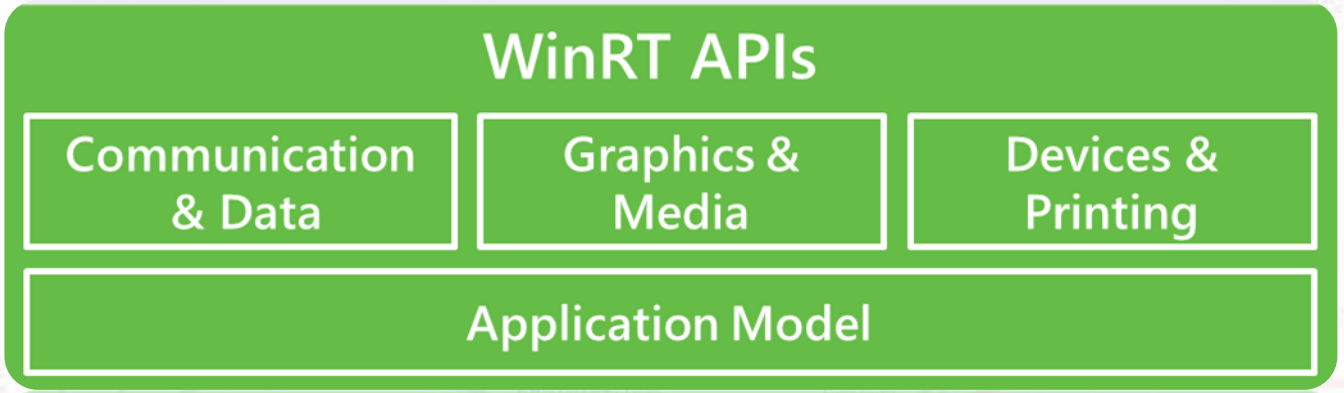



```
text:00404958 ; const JITDebuggingHost::CHost::`vftable'{for `IJITDebuggingHost2'}
text:00404958 ??_7CHost@JITDebuggingHost@@6BIJITDebuggingHost2@@@ dd offset ?QueryInterface@CHost@JITDebuggingHost@@UAGJABU_GUID@@PAPAX@Z
text:00404958                                         ; DATA XREF: .data:JITDebuggingHost::CHost JITDebuggingHost::CHost::s_Instance↓o
text:00404958                                         ; JITDebuggingHost::CHost::QueryInterface(_GUID const &,void * *)
text:0040495C                 dd offset ?AddRef@CHost@JITDebuggingHost@@UAGKXZ ; JITDebuggingHost::CHost::AddRef(void)
text:00404960                 dd offset ?Release@CHost@JITDebuggingHost@@UAGKXZ ; JITDebuggingHost::CHost::Release(void)
text:00404964                 dd offset ?JITAsLoggedInUser@CHost@JITDebuggingHost@@UAGJUtagCRASHING_PROGRAM_INFO@@@Z ; JITDebuggingHost::CHost
```

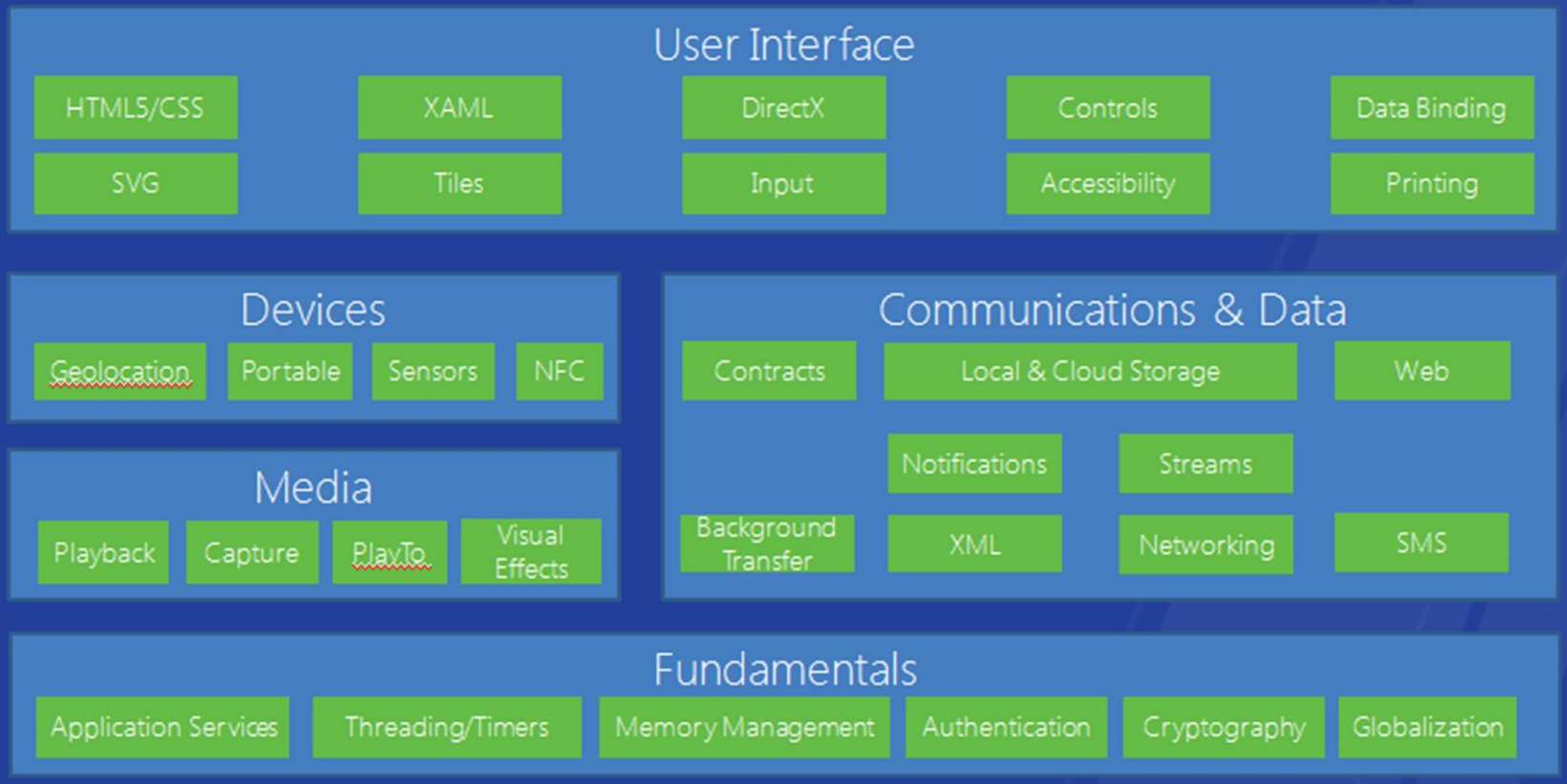
COM Interface Method Fuzzing

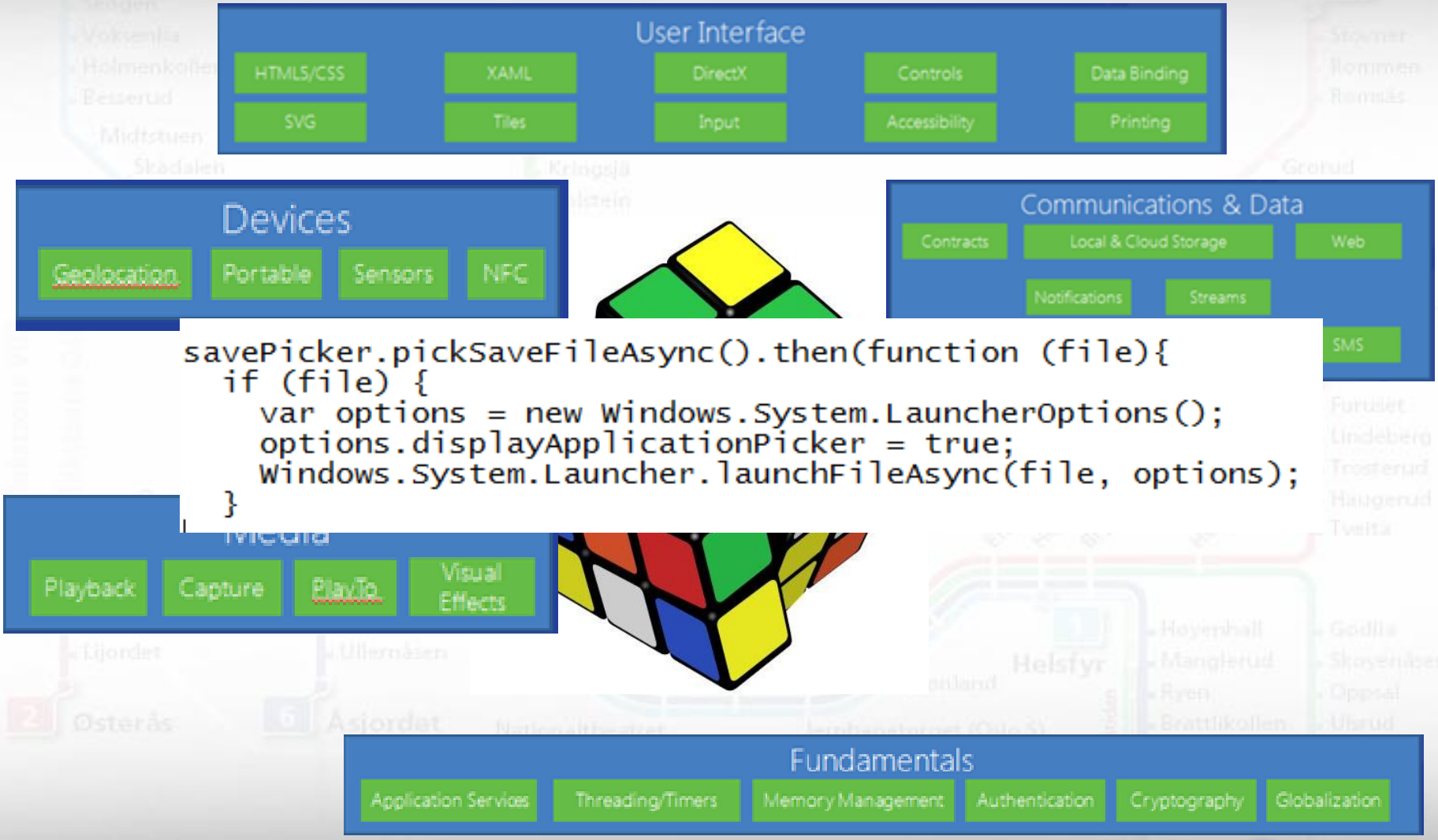


ATTACK WINRT API



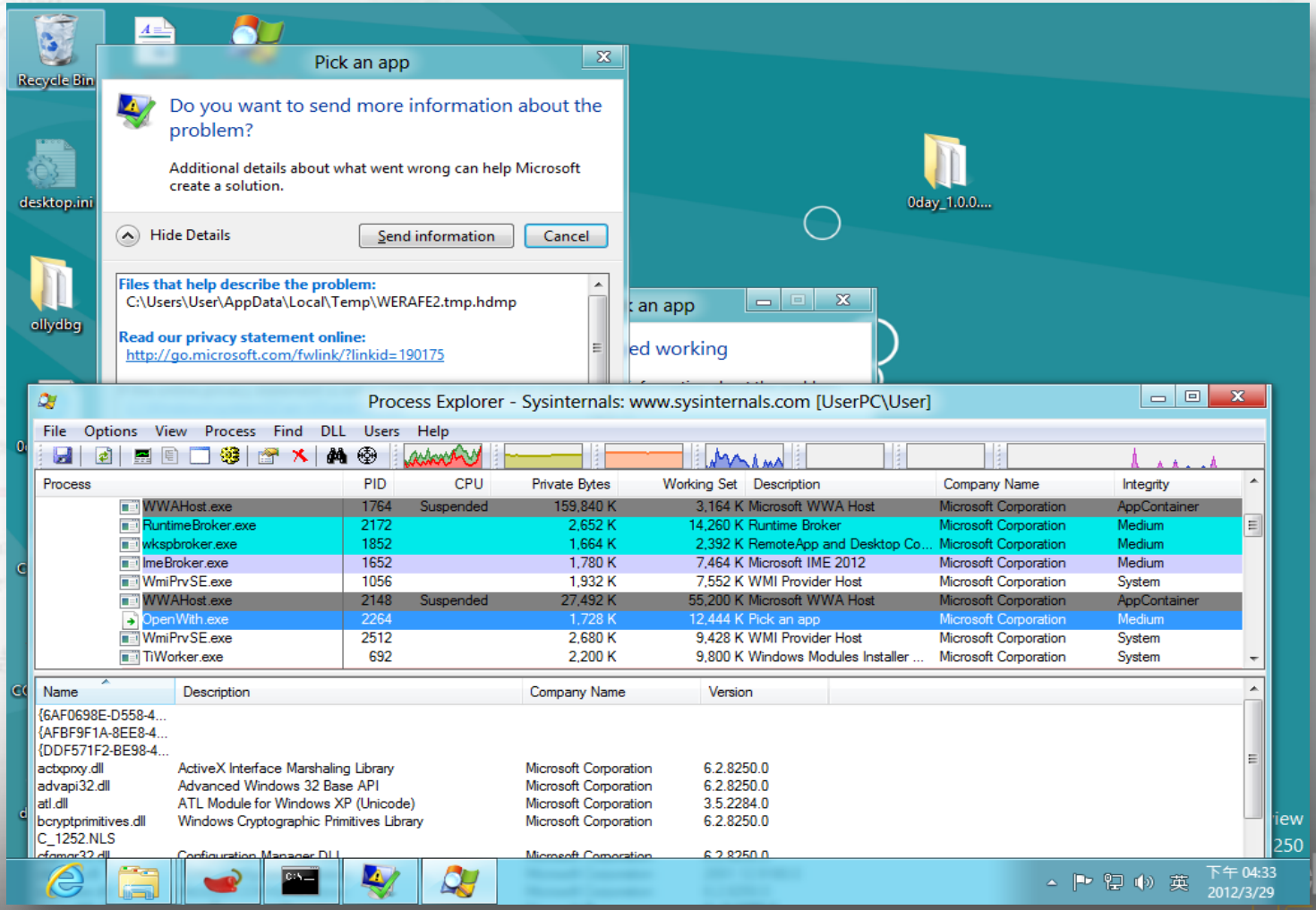
Metro style application APIs




User Interface
HTML5/CSS
XAML
DirectX
Controls
Data Binding
SVG
Tiles
Input
Accessibility
Printing
Devices
Geolocation
Portable
Sensors
NFC
Communications & Data
Contracts
Local & Cloud Storage
Web
Notifications
Streams
SMS
savePicker.pickSaveFileAsync().then(function (file){
if (file) {
var options = new Windows.System.LauncherOptions();
options.displayApplicationPicker = true;
Windows.System.Launcher.launchFileAsync(file, options);
}
Playback
Capture
PlayTo
Visual Effects
Fundamentals
Application Services
Threading/Timers
Memory Management
Authentication
Cryptography
Globalization

Discovered an Issue of a Broker Process

- OpenWith.exe (memory corruption)



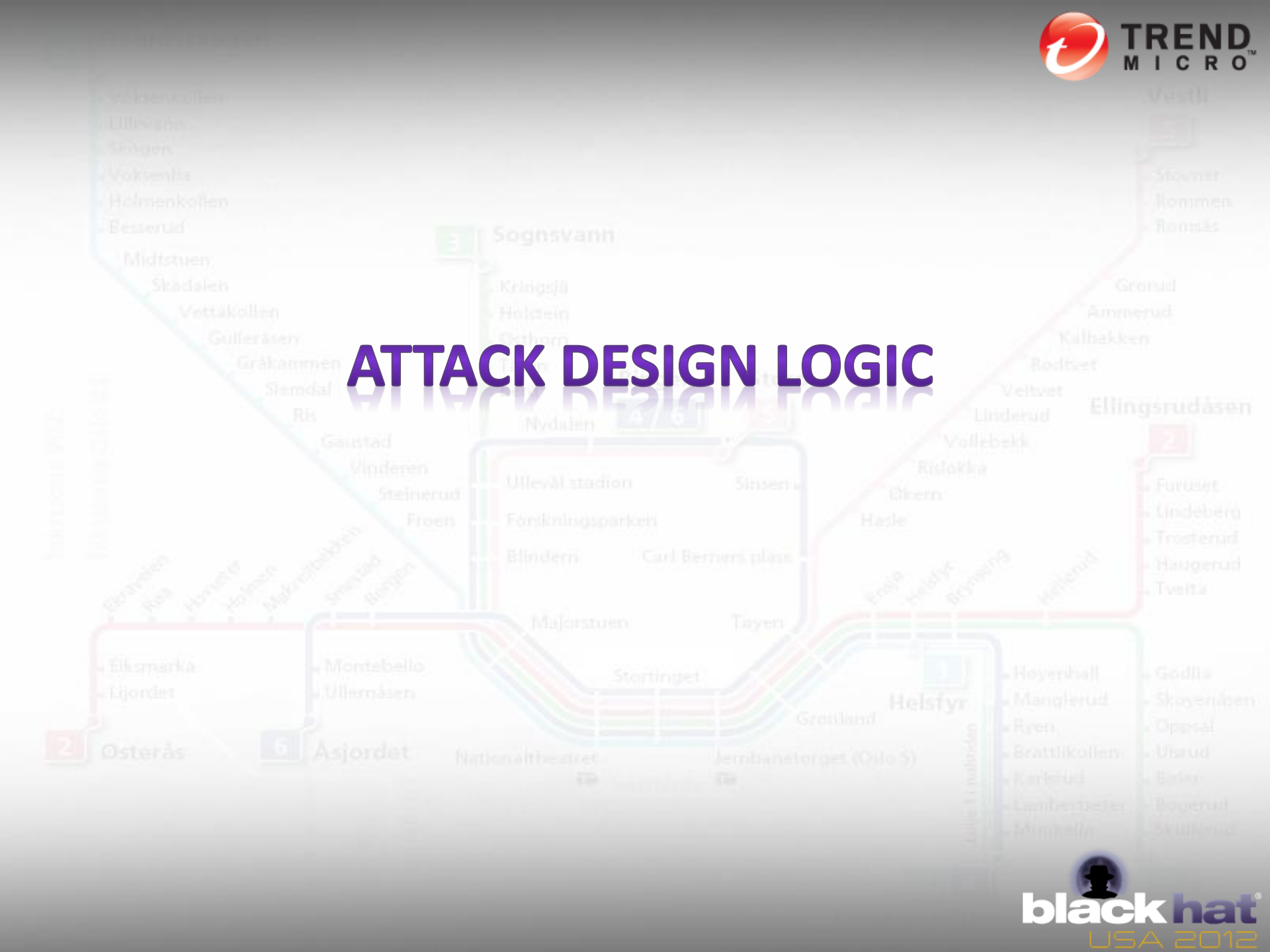
```
HostMachine\HostUser
Executing Processor
Debuggee is in User
Debuggee is a live
Event Type: Exceptic
Exception Faulting
Second Chance Except
Exception Sub-Type:

Faulting Instructio

Basic Block:
    70b35b6e mov ecx
       Tainted Input
    70b35b70 lea edx
    70b35b74 push edx
    70b35b75 push eax
       Tainted Input Operands: eax
    70b35b76 call dword ptr [ecx+18h]
       Tainted Input Operands: ecx, StackContents
```

```
70b35b74 push edx
70b35b75 push eax
   Tainted Input Operands: eax
70b35b76 call dword ptr [ecx+18h]
   Tainted Input Operands: ecx, StackContents

Exception Hash (Major/Minor): 0x1c2f2c0a.0x3205657c
```

```
Description: Data from Faulting Address controls Code Fl
Short Description: TaintedDataControlsCodeFlow
Exploitability Classification: PROBABLY_EXPLOITABLE
Recommended Bug Title: Probably Exploitable - Data from
```

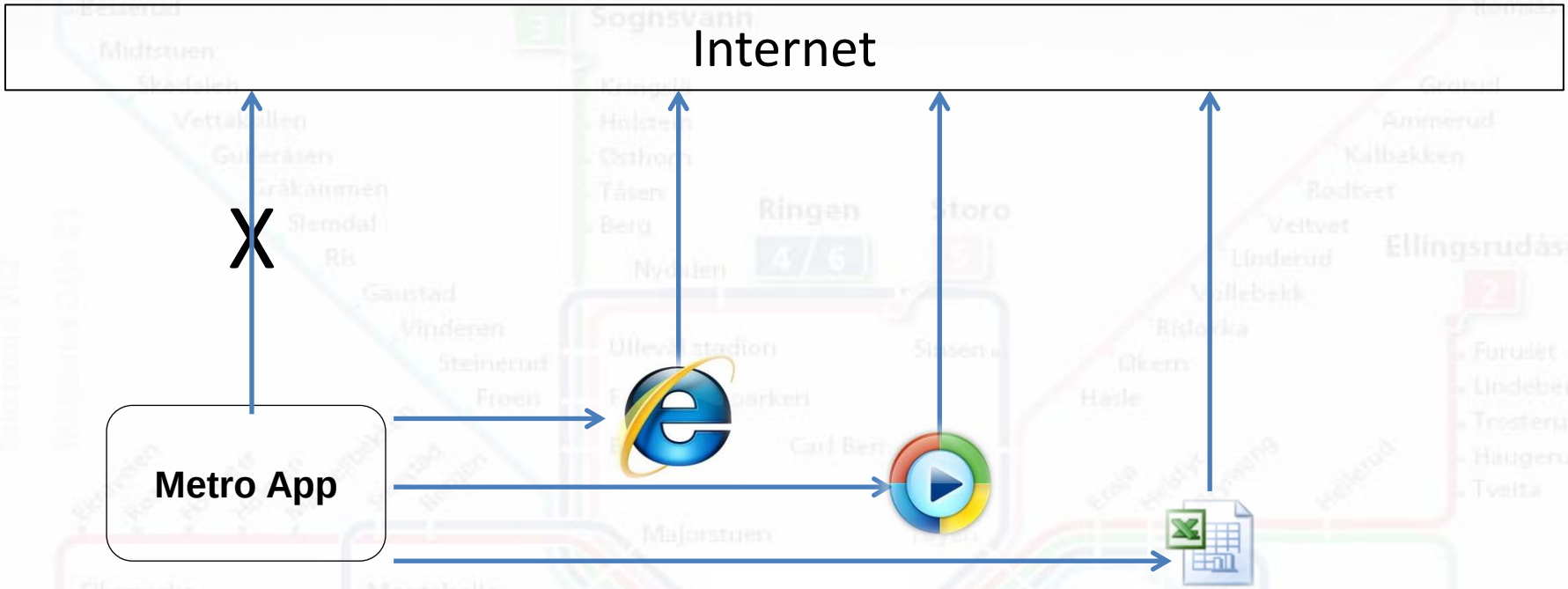
```
KERNEL32!BaseThreadInitThunk+0xe
ntdll!__RtlUserThreadStart+0x4a
ntdll!_RtlUserThreadStart+0x1c
Instruction Address: 0x0000000070b35b6e

Description: Data from Faulting Address controls Code Flow
Short Description: TaintedDataControlsCodeFlow
Exploitability Classification: PROBABLY_EXPLOITABLE
Recommended Bug Title: Probably Exploitable - Data from Faulting Address controls Code Flow starting at twinui!CImmersiveOp

The data from the faulting address is later used as the target for a branch.
```

ATTACK DESIGN LOGIC



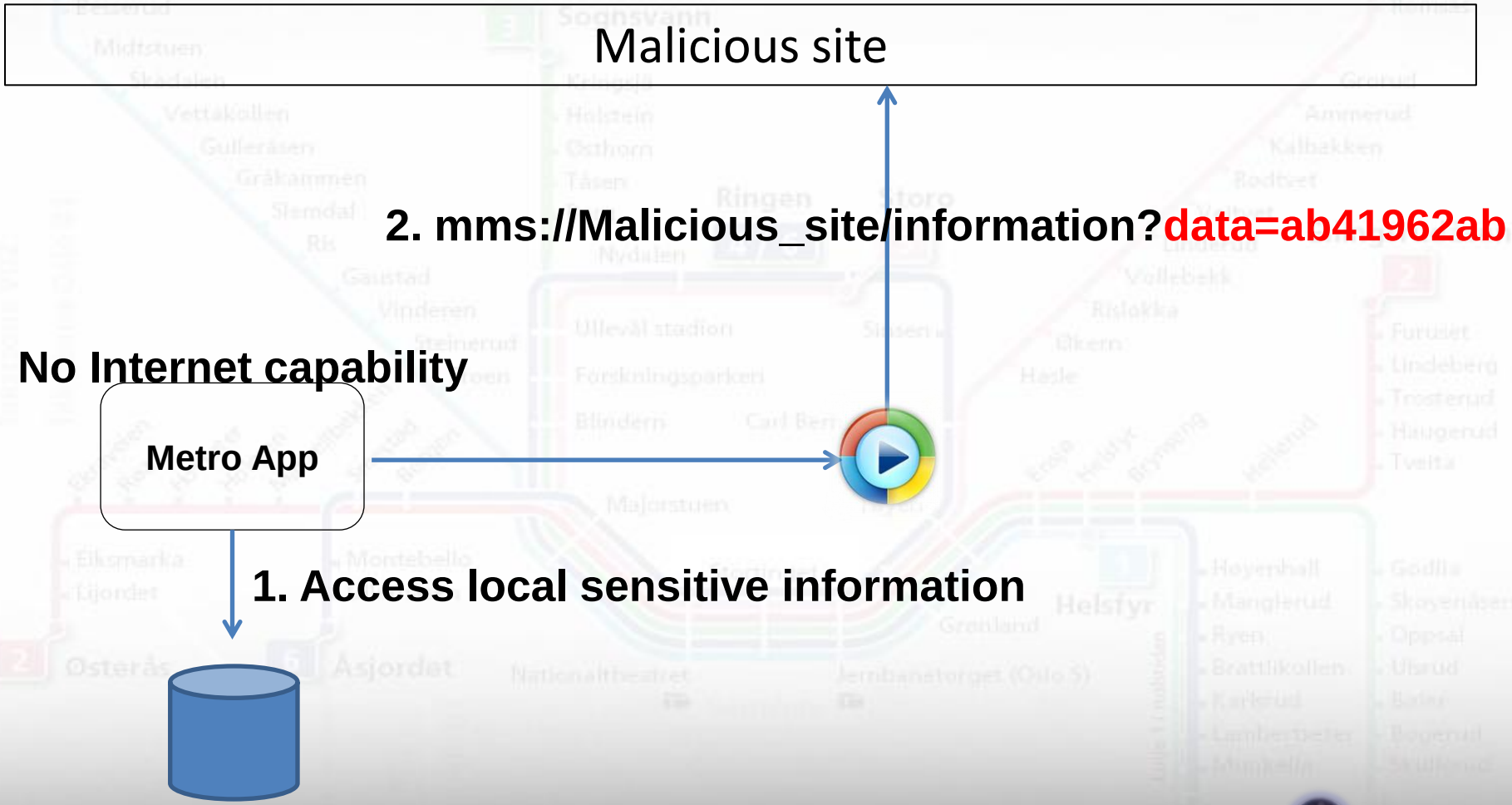
BYPASS INTERNET CONNECTION

Bypass Internet Connection Limitation



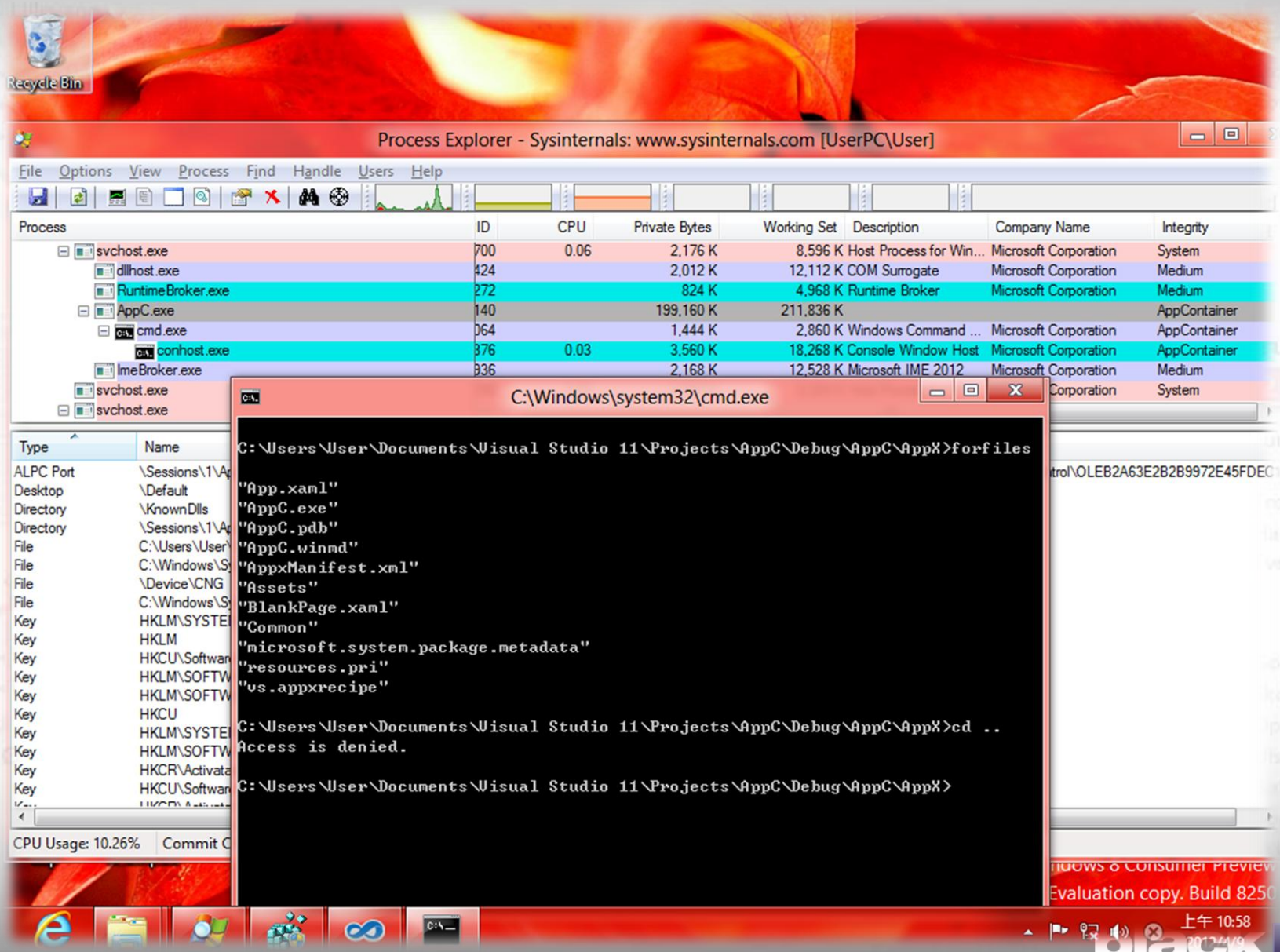
MSRC:
Such undesirable activities are highly detectable by either users or the AV industry, and once reported to Microsoft, we have the ability to remove the offending app from all user machines, thus protecting Windows 8 users.

Bypass Internet Connection Limitation

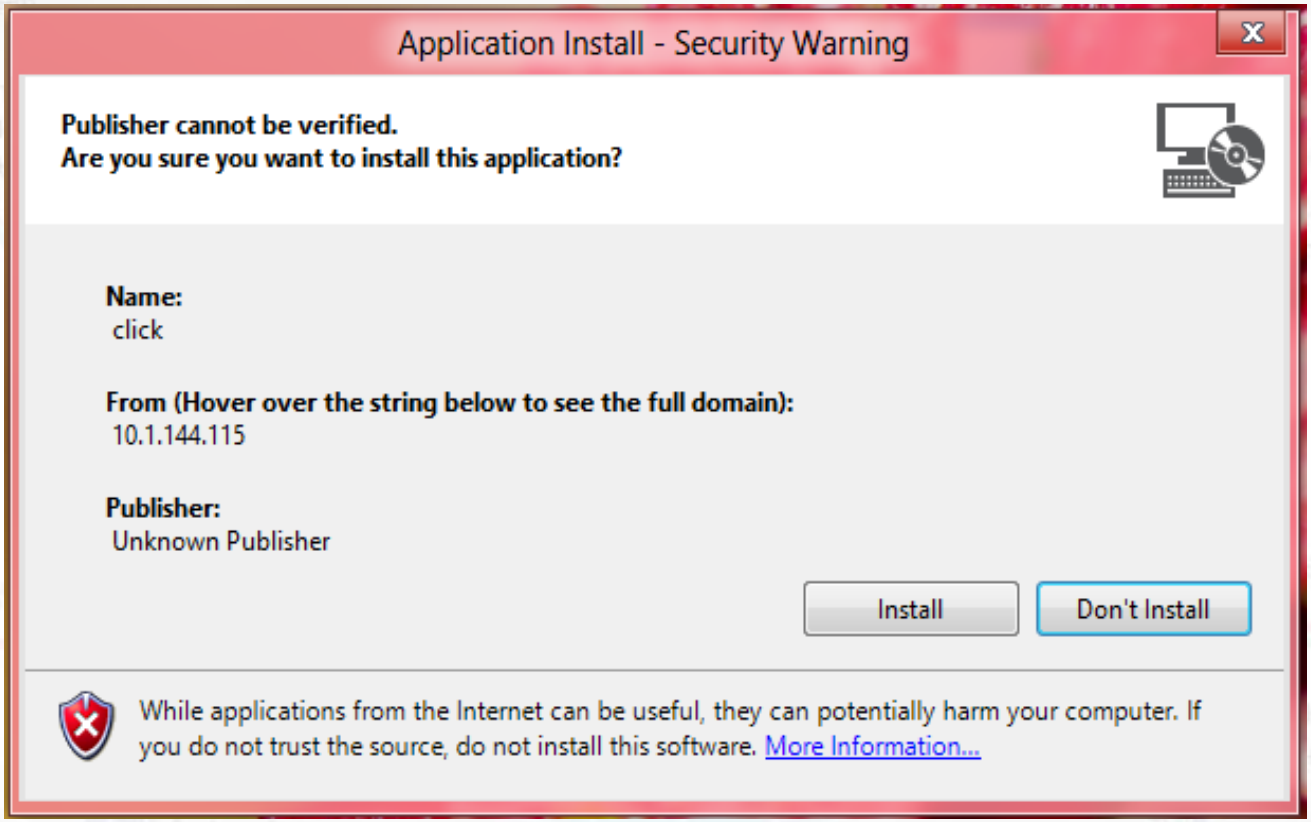


BYPASS LAUNCH PROGRAM LIMITATION

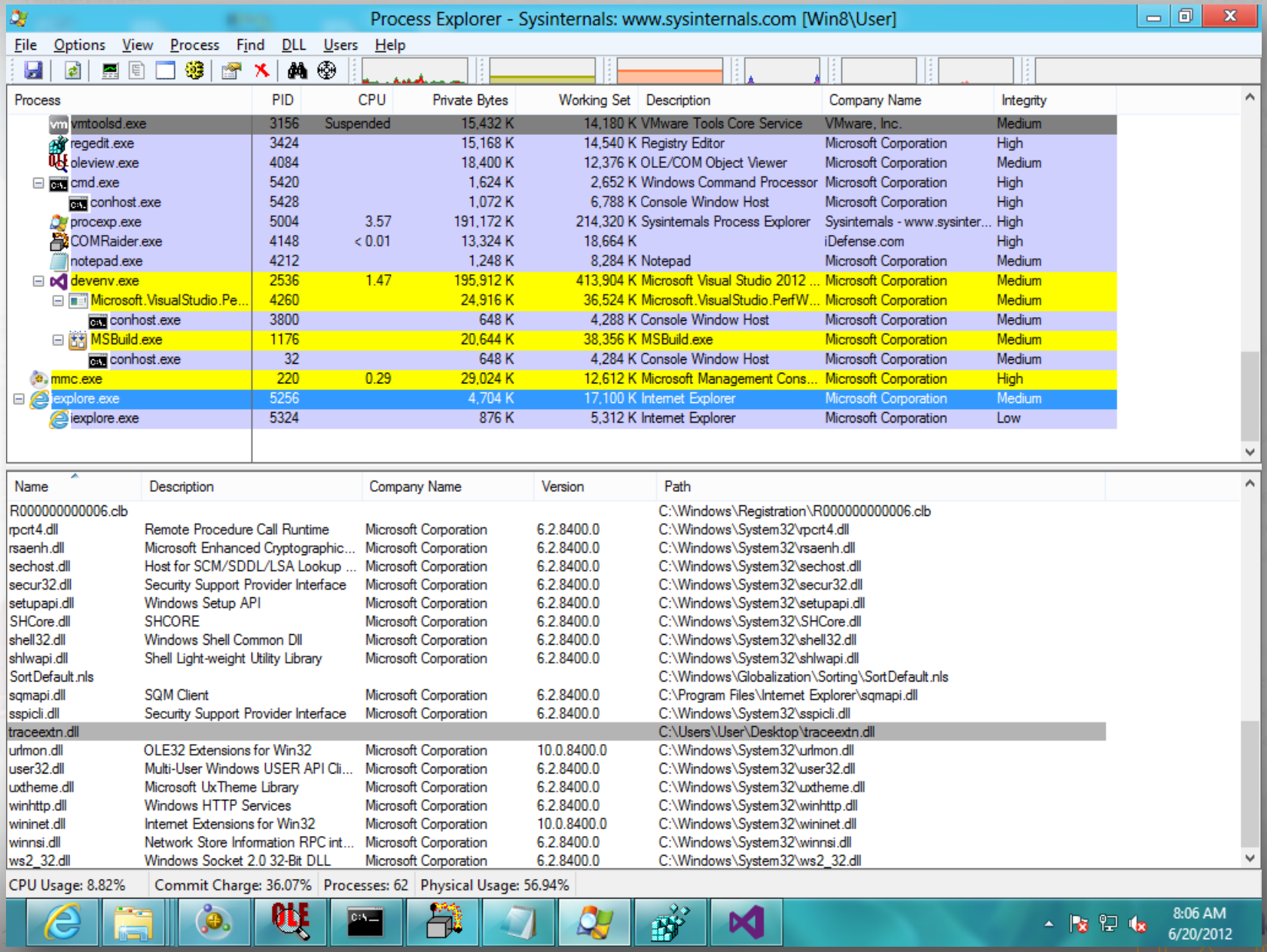
Inline ASM and Shellcode



ClickOnce package (.Application/.xbap) is executable



DLL Hijacking



MSRC:
(ClickOnce)
ClickOnce problem ***will be fixed in next Windows 8 release****.*

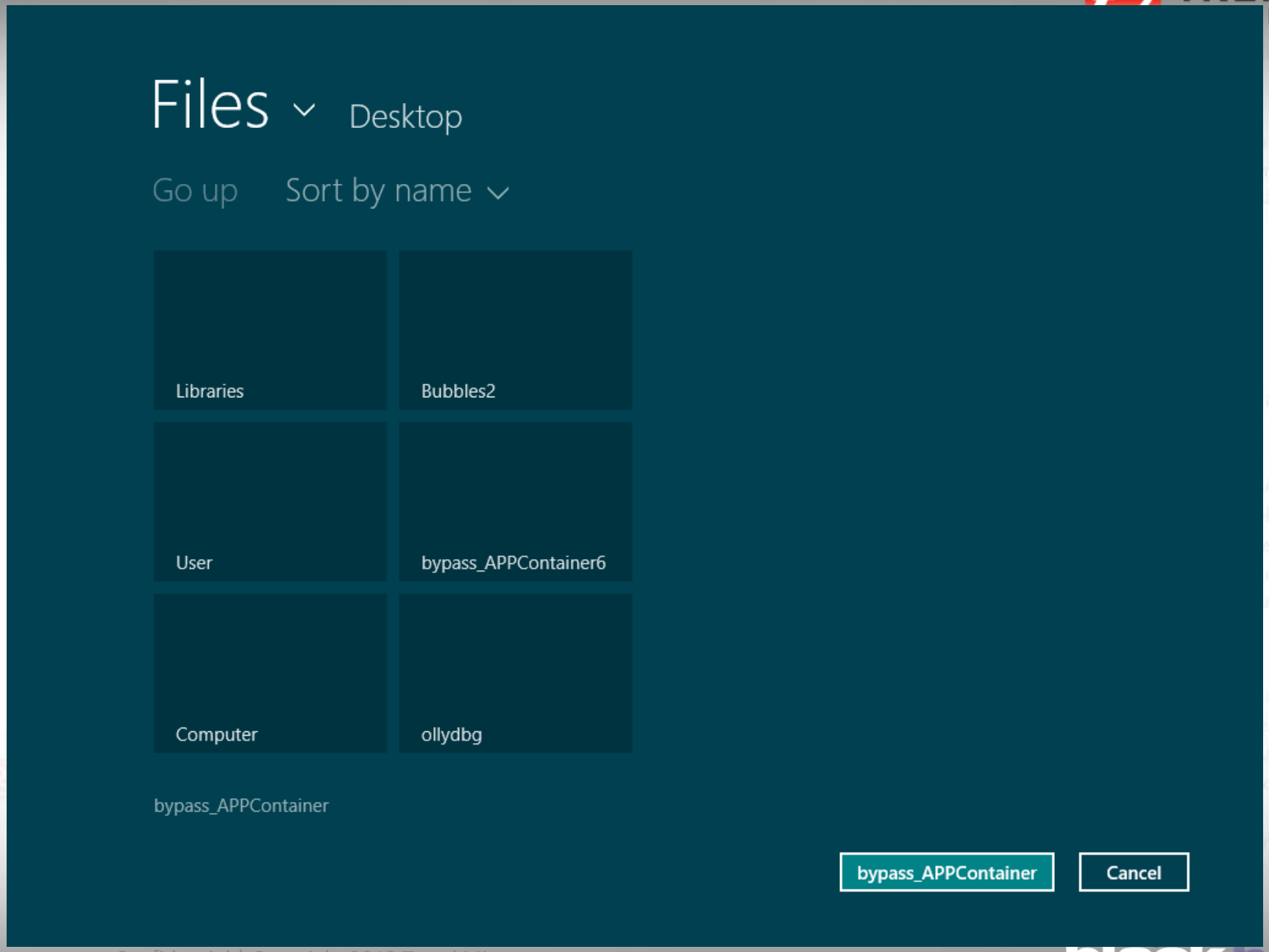
(DLL Hijacking)
We would consider this type of exploit a ***vulnerability in the desktop applications*** *rather than a vulnerability in the metro app or the platform. We continue to address DLL hijacking bugs in security updates as detailed in our security advisory for Insecure Library loading.*

BYPASS FILE/FOLDER ACCESS

Demo

FilePicker

- PickerHost.exe (the broker process)
  - The broker process
  - Medium permission
  - When user need to save / read files from some specific folder which is not specified in capability settings.
- Even you didn't grant file system access to App, the App still can use SavePickFile/PickFolder to let user choice folders they want to access, such as save a file in user-specified folders.
- After user clicking OK, the app can have full control of the folder with broker permission.


Files
Desktop
Go up
Sort by name
Libraries
Bubbles2
User
bypass_APPContainer6
Computer
ollydbg
bypass_APPContainer
bypass_APPContainer
Cancel

MSRC:

*This is a **deliberate feature**, and fully under the user's control. **Users should not click "ok" to the File picker dialog if they do not want the app to have access to that folder tree**. We consider this under the user's control and as such do not view it as a threat. .*

Conclusion

- Introduced
  - Security design of AppContainer
  - The methodology of Metro style app vulnerability discovery
  - The issues we have discovered.
- Security v.s. convenience, a never solved problem?
- Do users really know what will happen after clicking ‘OK’?

Thanks!

http://exploitspace.blogspot.com/

Contact: (nanika_pan|tt_tsai)@trend\.com\.tw