

Exploitation of Windows 8 Metro Style Apps

The Subway Line 8

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

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)

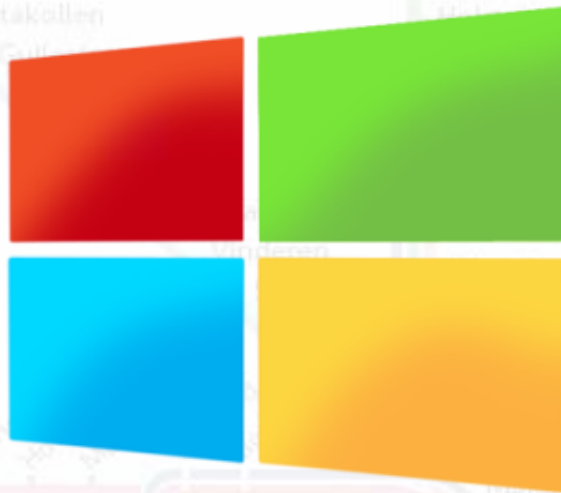
- Leader of an advanced threat research team.
- Research topics:
 - New security technology
 - Advanced Persistent Threat
 - Malicious document
 - Malware auto-analyzing system (sandbox technologies)
 - Malware detection
 - System vulnerability and protection
 - Mobile security
- Talks and speeches
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

HITCON 2012

NEXT GENERATION THREATS

新世代的攻擊威脅

CHROOT Security Group



Windows® 8

- 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

The properties of the deployment package for your app are contained in the app manifest file. You can use the Manifest Designer to set or modify one or more of the properties.

Declarations	Content URIs	Packaging
Application UI		Capabilities
Capabilities: ☒ Documents Library Access ☐ Enterprise Authentication ☐ Home or Work Networking ☐ Internet (Client & Server) ☐ Internet (Client) ☐ Location ☐ Microphone ☐ Music Library ☐ Pictures Library Access ☐ Proximity ☐ Removable Storage ☐ Shared User-Certificates ☐ Text Messaging ☐ Videos Library Access ☐ Webcam	Description: Enables adding, changing, or deleting files in the documents libraries that are defined by the file type association handler declarations. Applications cannot access document libraries on HomeGroup computers. More information	

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

Home > News & weather > News

Overview Details Reviews

USA TODAY was installed.



Write a review



233 ratings

Free

You own this app.

When you install an app, you agree to the

This app has permission to use:
Location
Your Internet connection

Age rating: 12+

This app has permission to use:
Location
Your Internet connection

Age rating: 12+

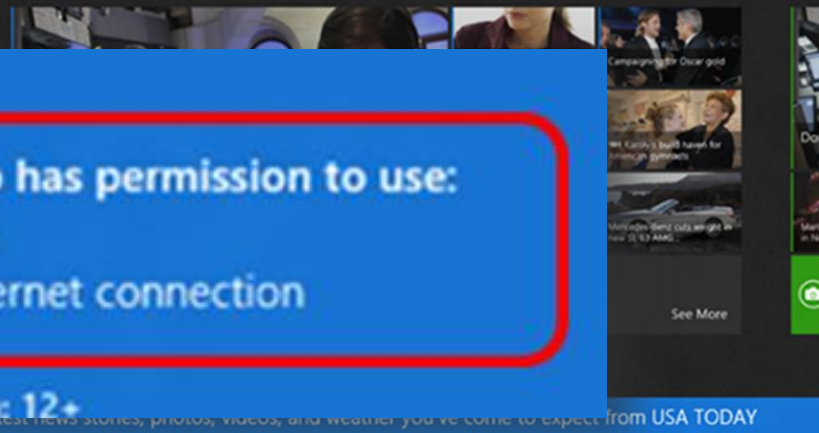
Developer: USA TODAY

© 2012 USA TODAY, a division of Gannett Satellite Information Ne...



New York
New York 43°

News



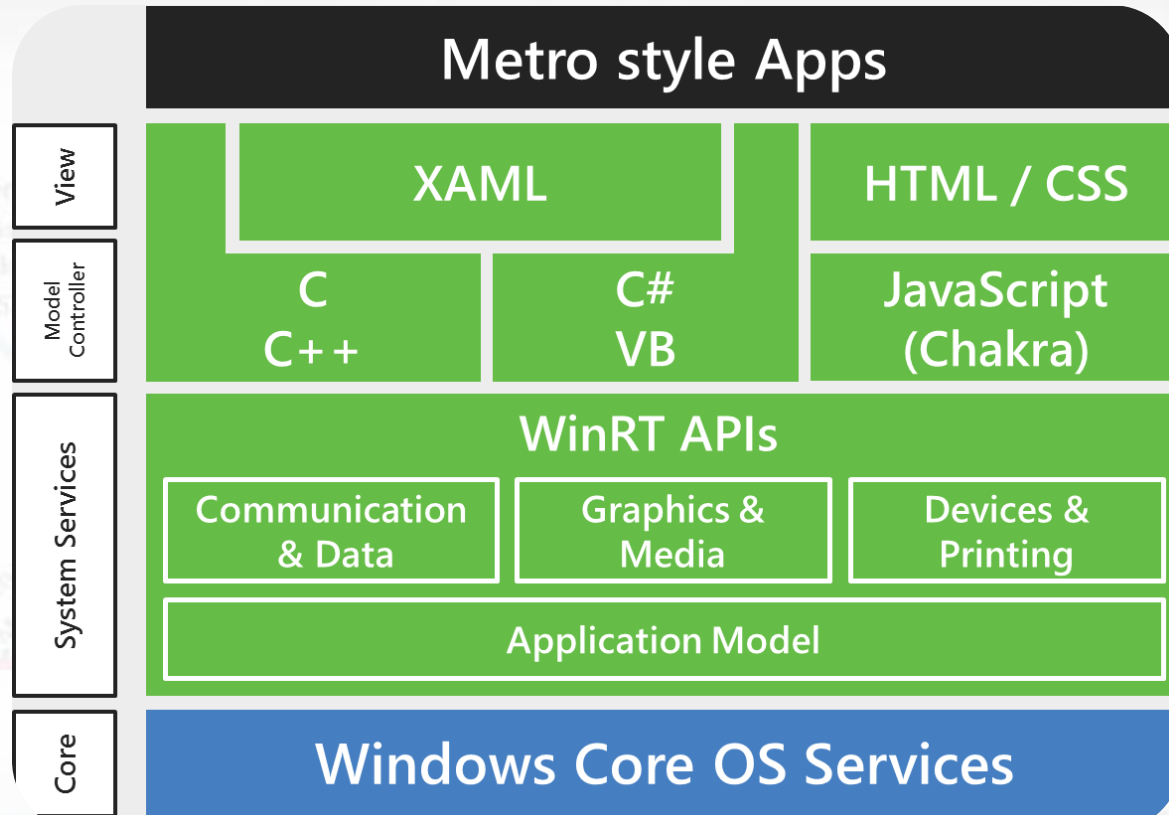
Description

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

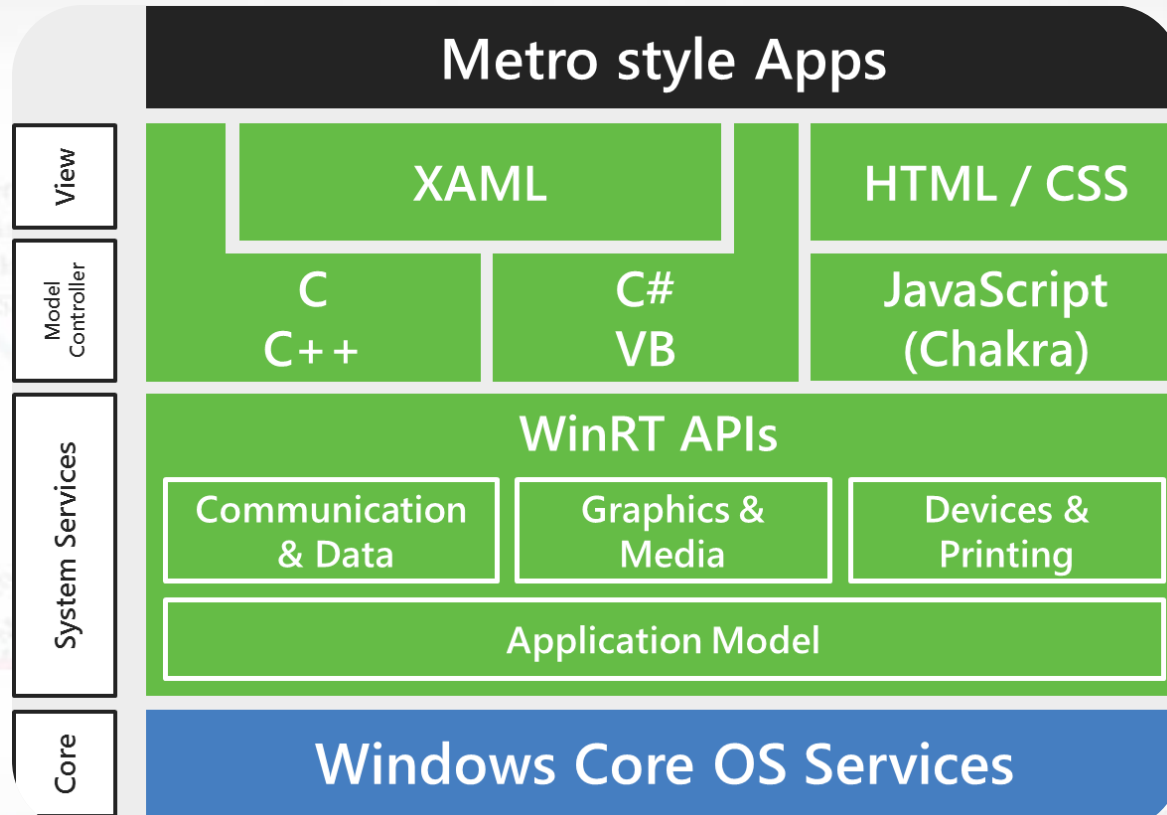


Source: <http://blogs.msdn.com/b/b8/archive/2012/02/09/building-windows-for-the-arm-processor-architecture.aspx>

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



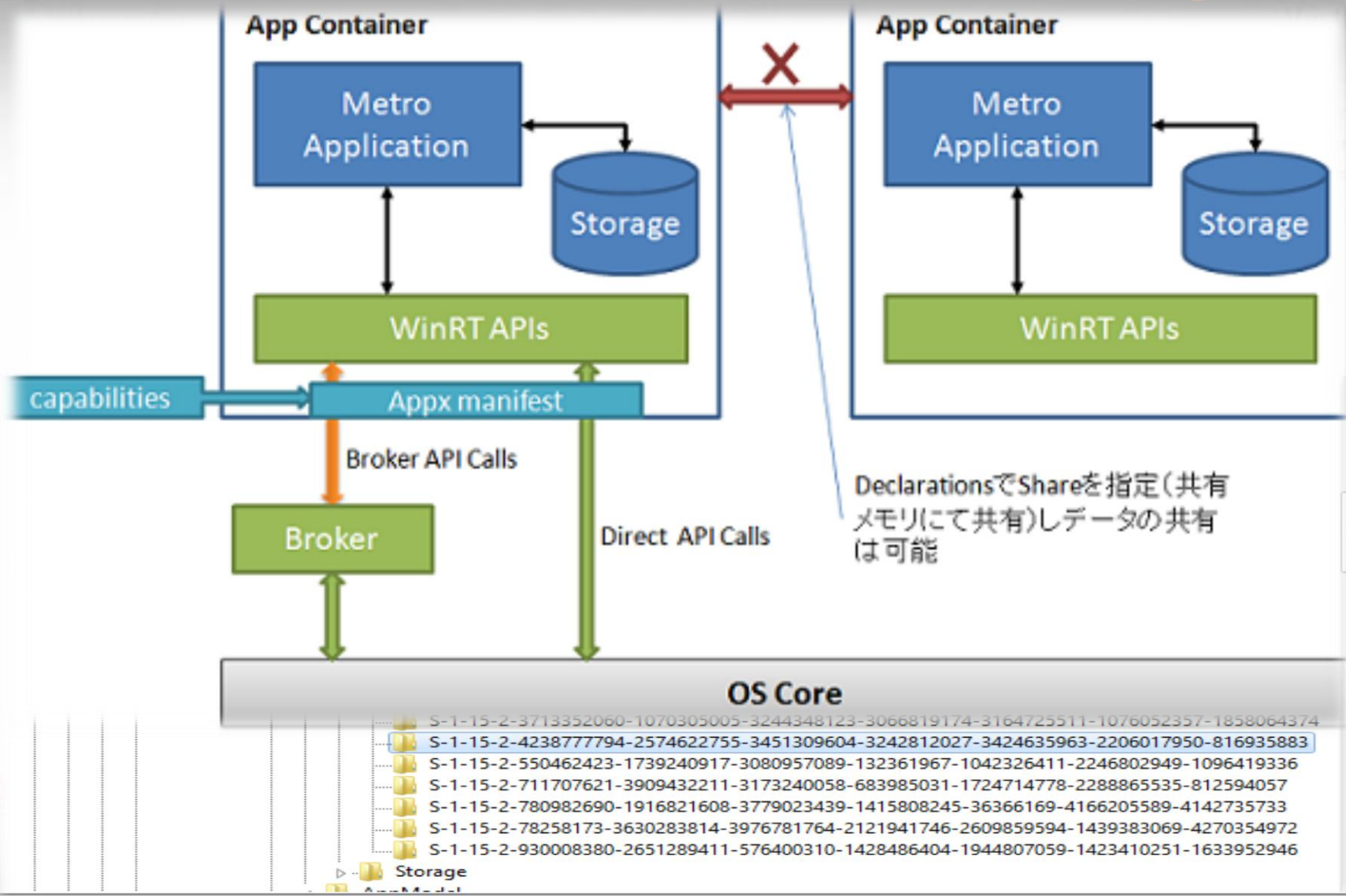
APP CONTAINER



<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



Computer\HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-



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

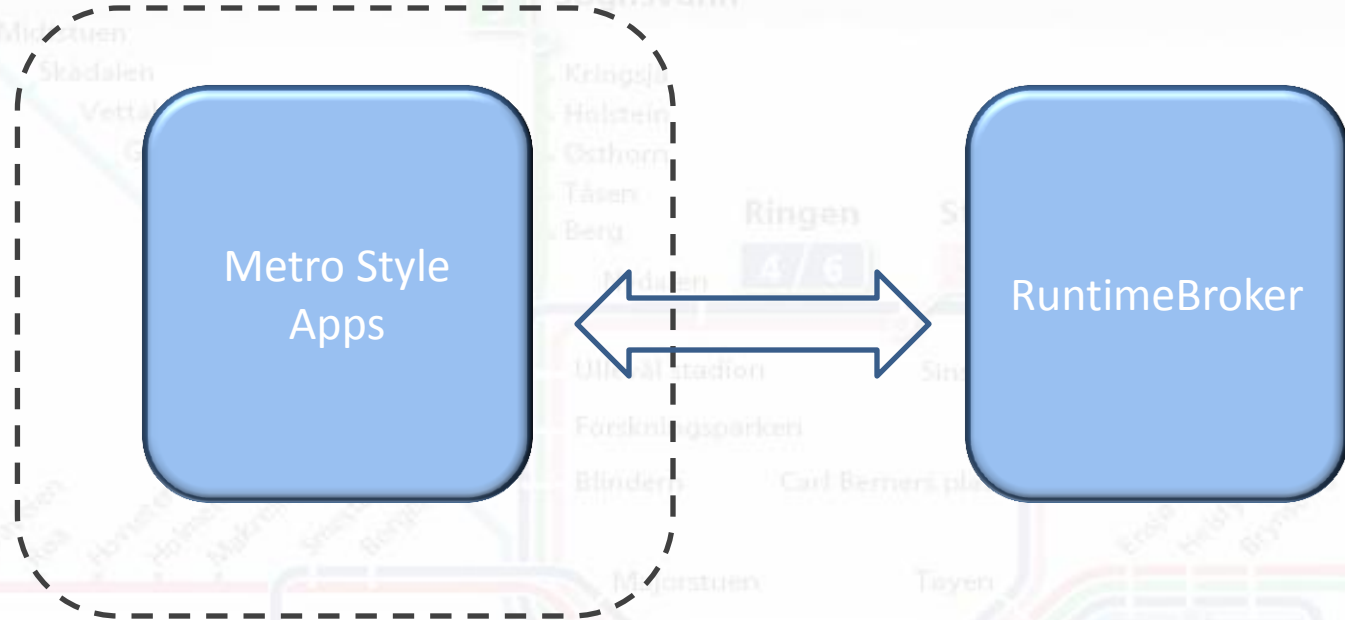
Previous Works on Sandbox Bypassing

- 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



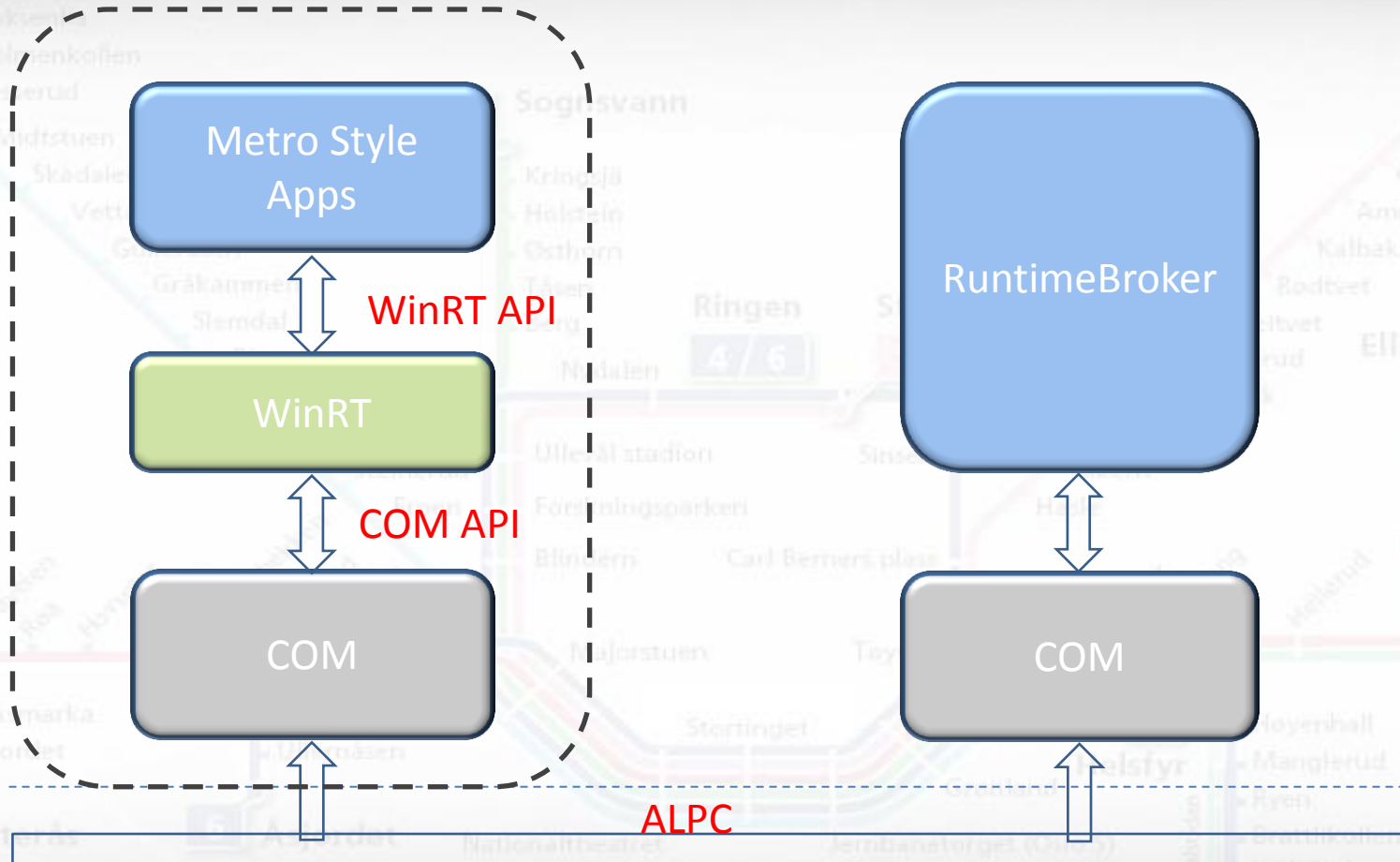
Find the Target



Metro Style
Apps

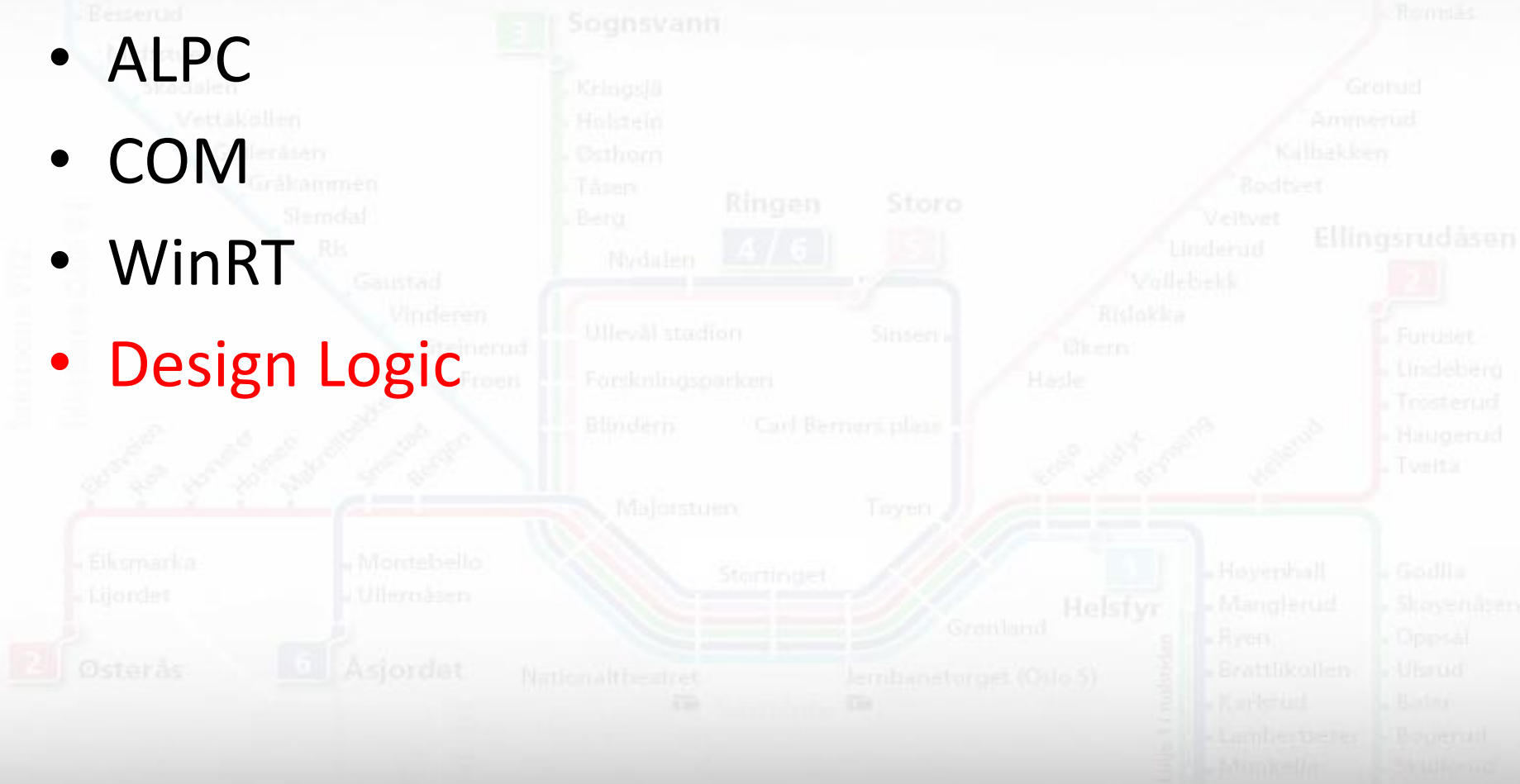
RuntimeBroker

Attack Vectors



AppContainer Sandbox Attack Vectors

- ALPC
- COM
- WinRT
- Design Logic



DEBUG OF ALPC COMMUNICATION

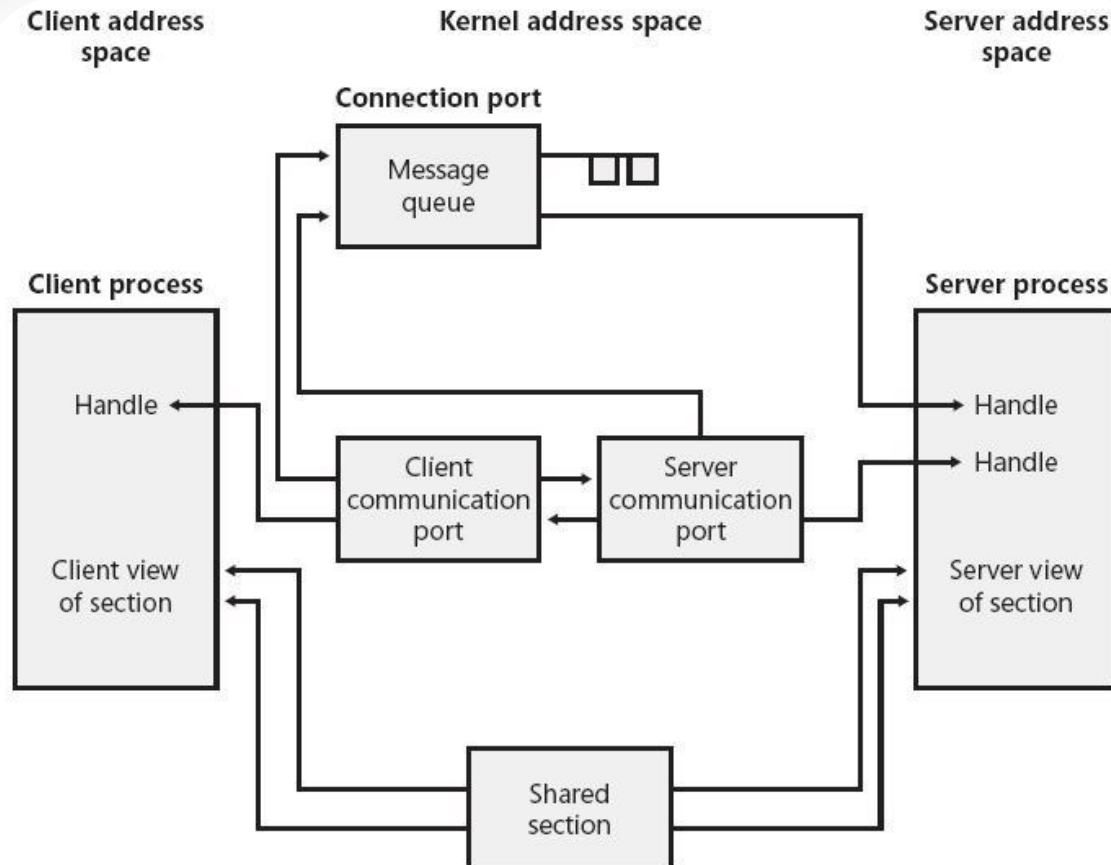
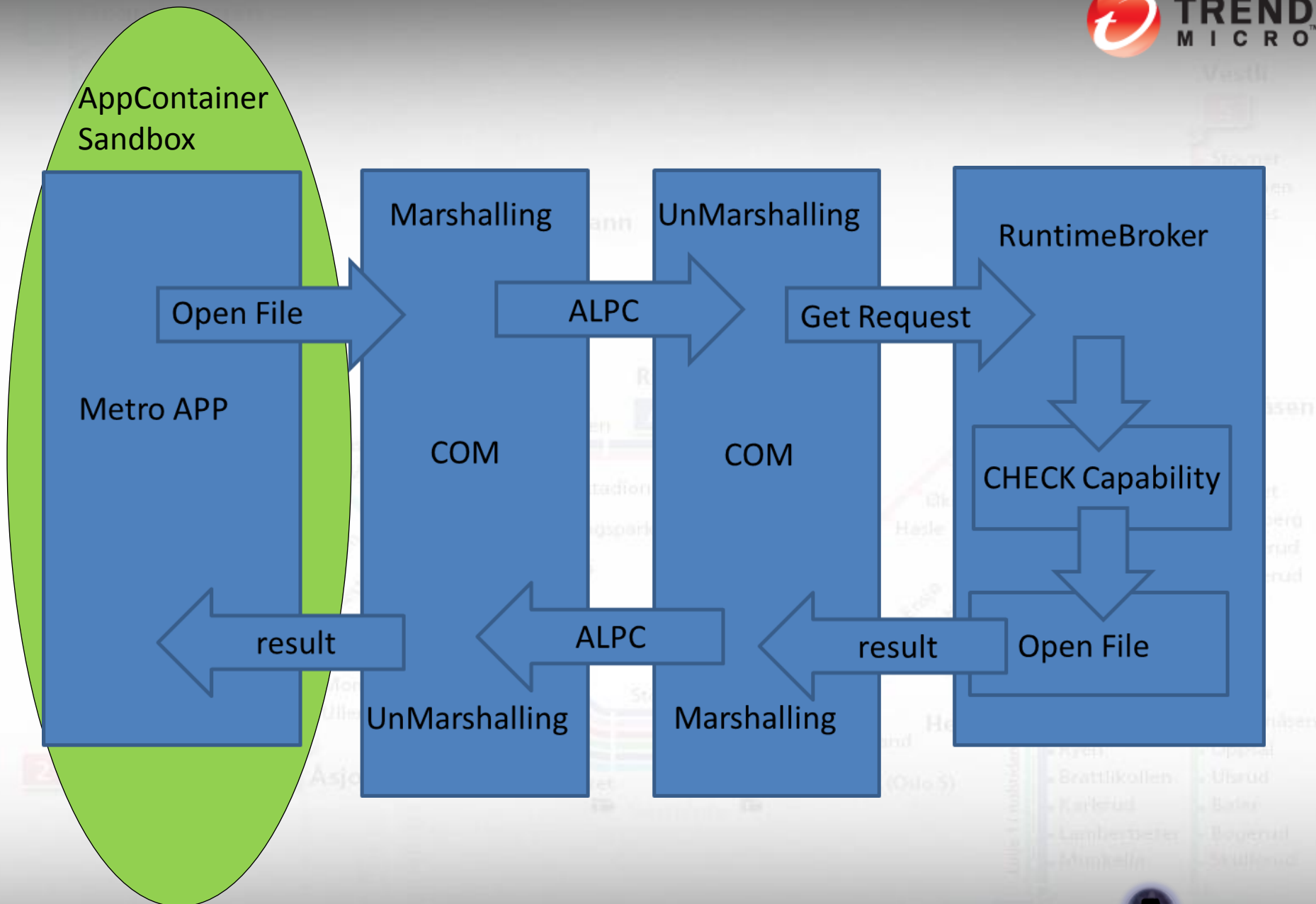


FIGURE 3-27 Use of ALPC ports

FIGURE 3-27 Use of ALPC ports



!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(@$teb+20),poi(esp+0x4),poi(esp+0x8),poi(esp+
0xc),poi(esp+0x10),poi(esp+0x14),poi(esp+0x18),poi(esp+0x1c),poi(esp
+0x20);.if(poi(esp+c)!=0){.printf "send:\";dt _PORT_MESSAGE
poi(esp+c);db poi(esp+c) |
(poi(poi(esp+c))&0xffff)+0x18;gc;}.if(poi(esp+0x14)!=0){r @$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 @$t0 | @$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+0  
x18),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+0  
x18),poi(esp+0x1c),poi(esp+0x20),poi(esp+0x24); "
```

ALPC Analysis Flow

.logopen "metroapp.txt"



Hook `nt!NtAlpcCreatePort`



Open Metro App



Hook

`ntdll!NtAlpcSendWaitReceivePort`

ncalrpc:[\\Sessions\\1\\AppContainerNamedObjects\\S-1-15-2-1115239912-5888679-3094415206-3103815194-10819155-2778485781-2267460753\\RPCControl\\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 .....
00bfb698 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
00bfb6a8 00 00 00 00 00 0a 00 00 00-03 00 00 00 00 00 .....
00bfb6b8 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 00-00 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
```

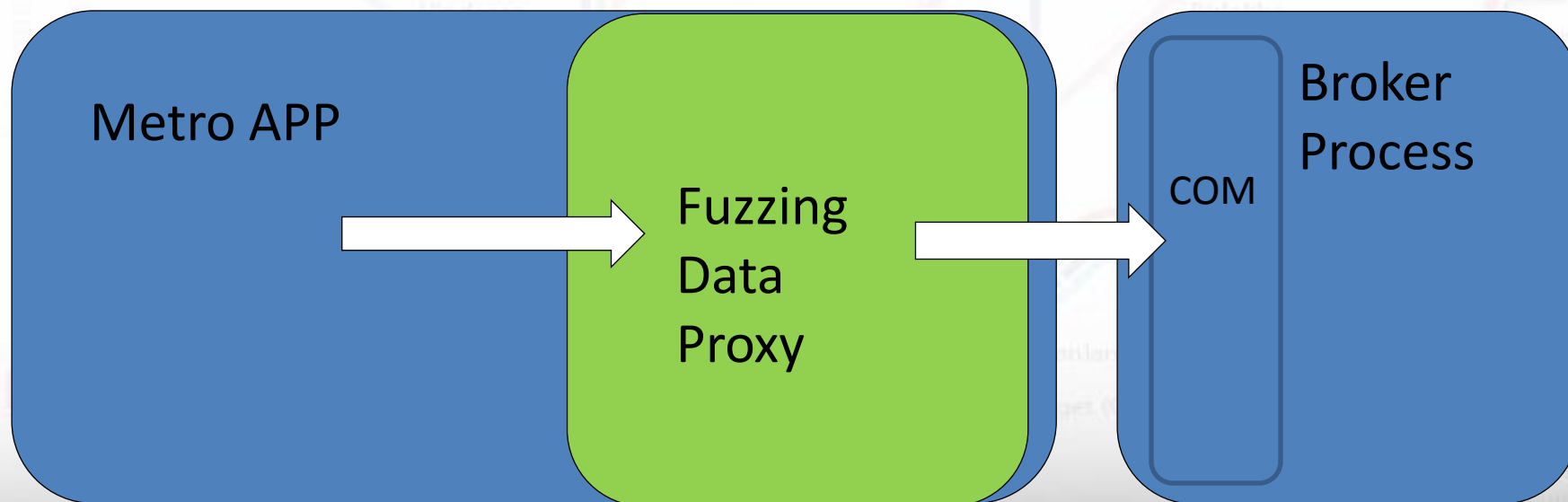
Name	Type	Data
(Default)	REG_SZ	(value not set)
ActivatableClassId	REG_SZ	App.wwa
PackageMoniker	REG_SZ	c000053d-77bc-4b2f-a138-db89d0eab2bf_1.0.0.1_neutral_4sdae...

RuntimeBroker

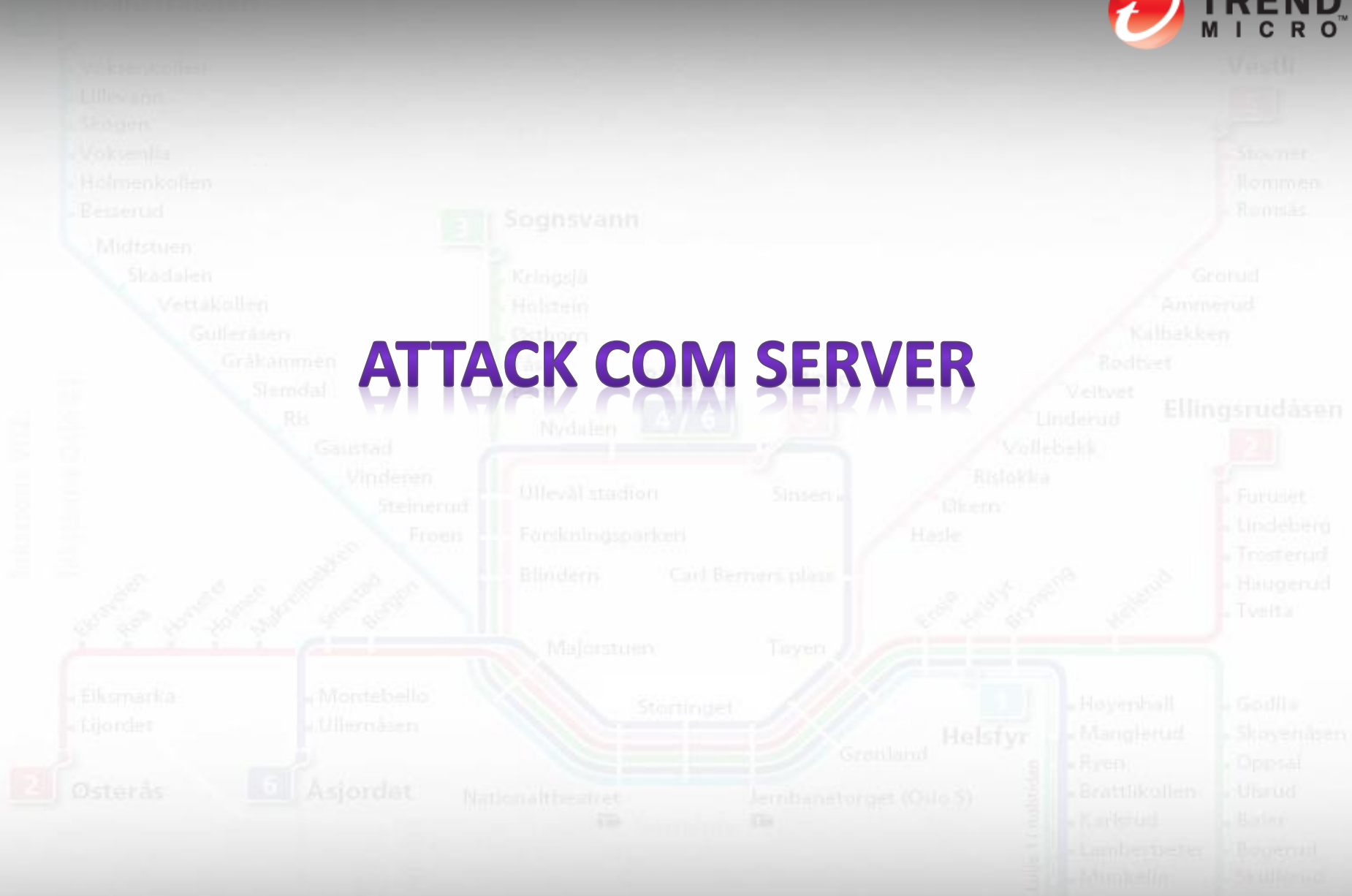
- # IRuntimeBroker

Fuzzing ALPC communication

- Inline ASM
- Hook `ntdll!NtAlpcSendWaitReceivePort`
- Modify Send Fuzzing Data



ATTACK COM SERVER



Windows 8 COM

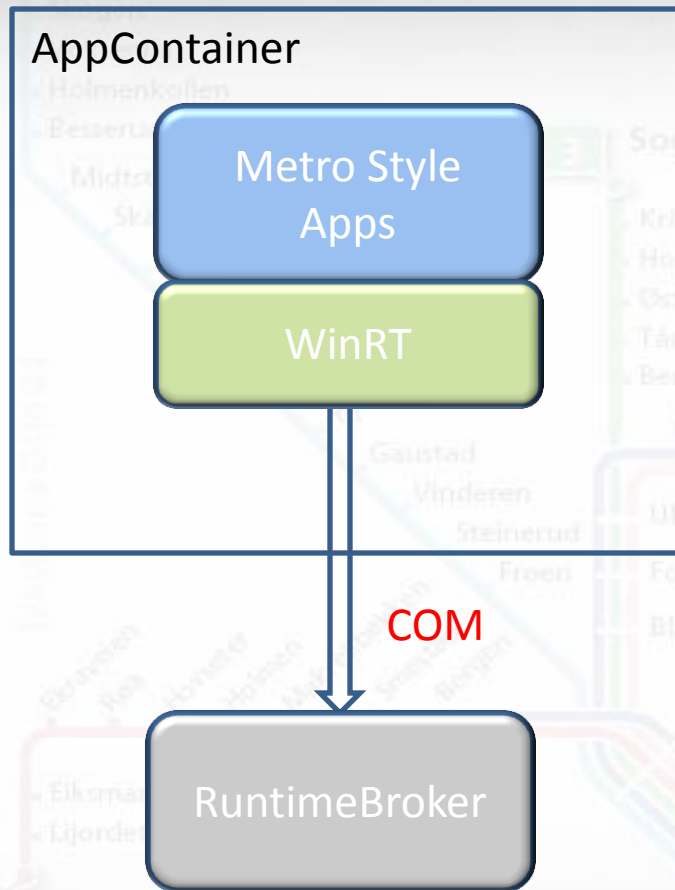
- InInitOrder.blink – kernelbase.dll (instead of kernel32.dll)
- OLE32.dll(Win2000->Win7)
- ComBase.dll (Windows 8)

(nFunctions)	Dword	Word	Dword	szAnsi
0000011D	000BB0E0	011C	000EE74D	RoOriginateError
0000011E	000BB0E6	011D	000EE75E	RoOriginateErrorW
00401020	. 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
00000122	000BB085	0121	000EE7D6	RoReportCapabilityCheckFailure
00000123	000BB7FD	0122	000EE7F5	RoResolveRestrictedErrorInfoReference
00000124	00032F5D	0123	000EE81B	RoRevokeActivationFactories
00000125	000BAC12	0124	000EE837	RoSetErrorReportingFlags
00000126	000BB247	0125	000EE850	RoTransformError
00000127	000BB11D	0126	000EE861	RoTransformErrorW
00000128	00032B9C	0127	000EE873	RoUninitialize
00000129	000331AB	0128	000EE882	RoUnregisterForApartmentShutdown

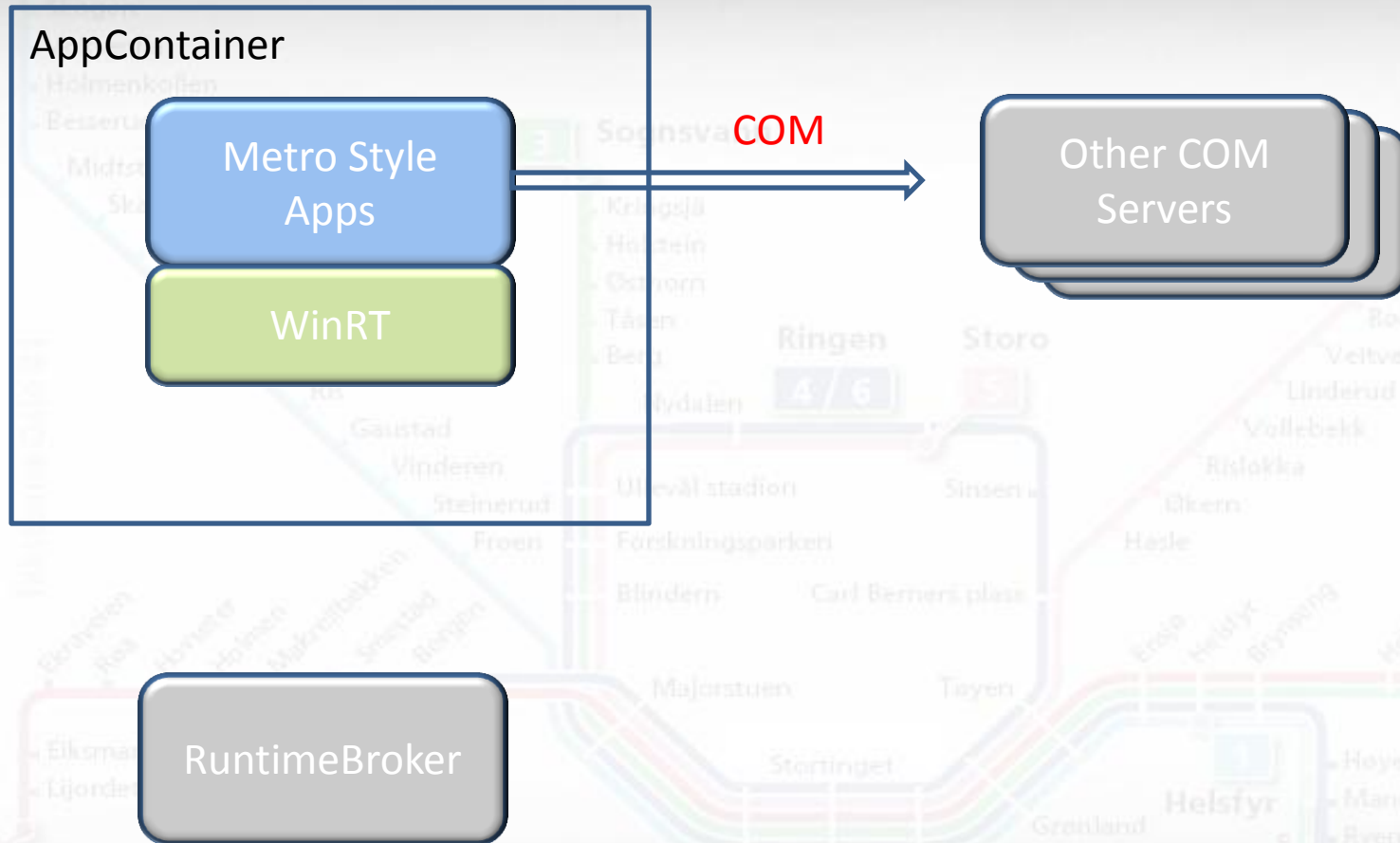
Purpose of COM Testing

- 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

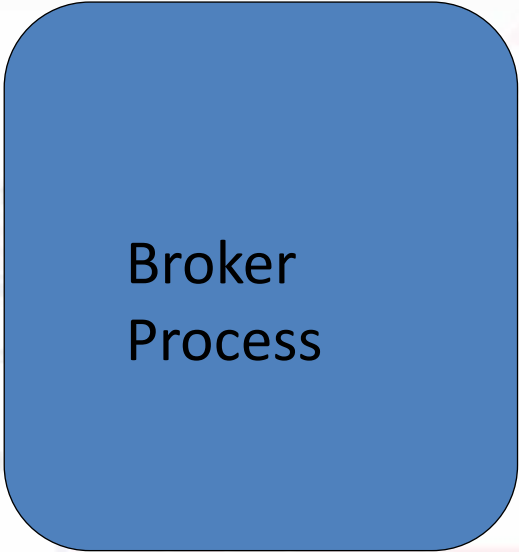


The Target – Privilege

 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
- ...



Broker
Process

The Target – Available COM

COMView				
File Edit View Special Help				
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-3D11968423D3}	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\MSpellCheckingHos...	
{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-D5F5-4F95-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...	Tablps.TextContrib
{4545dea0-2dfc-4906-a728-6d986ba399a9}	Thumbnail Extraction Host Class	LocalServer32	%SystemRoot%\System32\ThumbnailExtractio...	
{16A18E86-7F6E-4C20-AD89-4FFCDB7A96A}	TPM Virtual Smart Card Manager	LocalServer32	"%SystemRoot%\System32\Tpm\scMgrSrv.exe...	
{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-4347-8A35-6A4533254A9D}	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\vdslldr.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

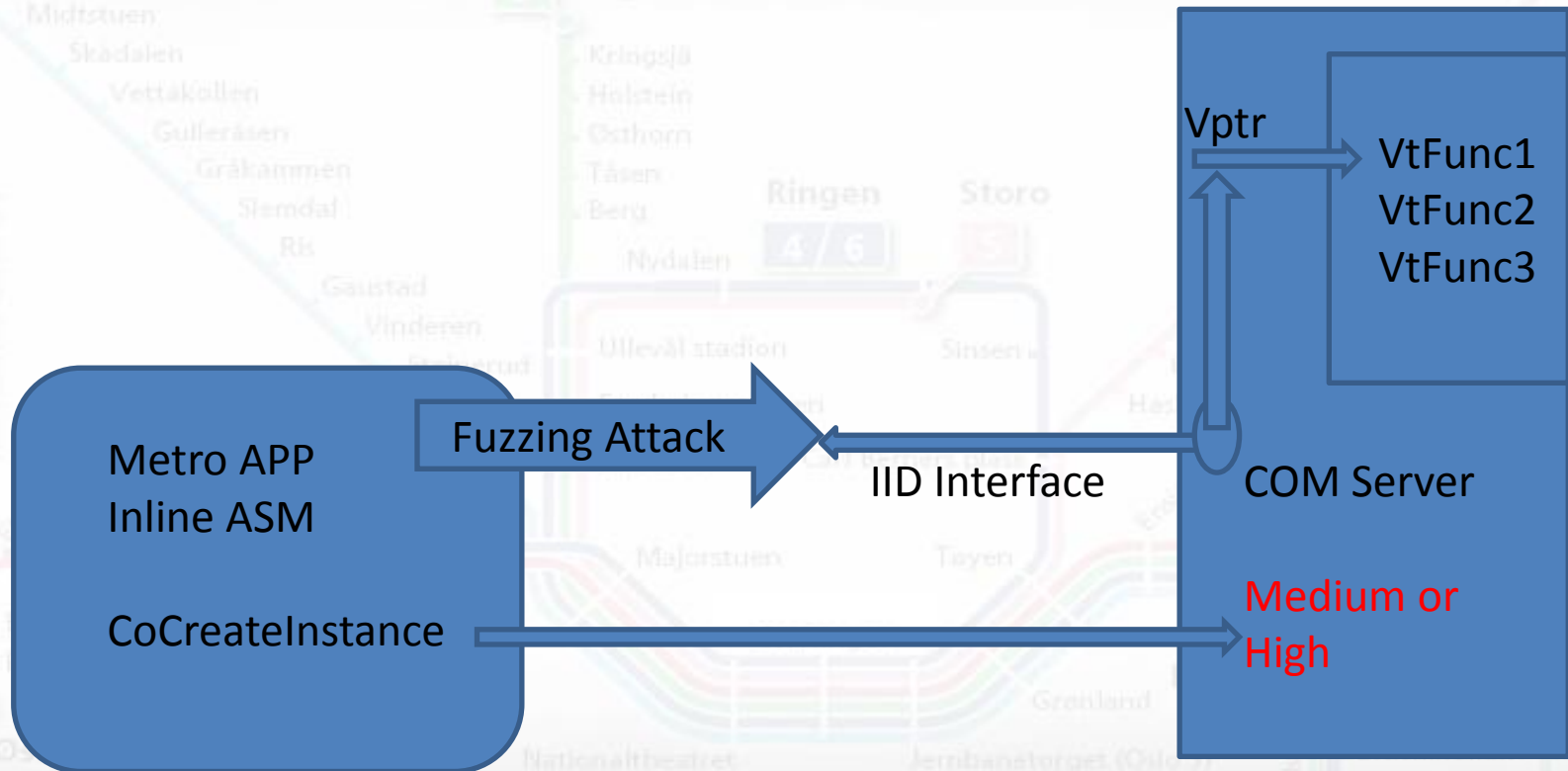
{de50c7bb-faa7-4a7f-ba47-bf0efcfe433d} <no name>
{DE50C7BB-FAA7-4A7F-BA47-BF0EFCFE433D}

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

Object: UIHost Class

IID	Name	Addr Interface	Addr VT able
{00000000-0000-0000-C000-000...	IUnknown	002C03C0	7753B1F4
{00000020-0000-0000-C000-000...	IMultiQI	002C03C0	7753B1F4
{0000013D-0000-0000-C000-00...	IClientSecurity	002C039C	7753B258
{00020400-0000-0000-C000-000...	IDispatch	0022BE34	757CC150
{11C4304D-0FAA-4C31-8BDD-4...	IHostWindow2	0022BBAC	6F8ED068
{37C994E7-432B-4834-A2F7-DC...	ITipInvocation	0022BD14	6F8ED0B4
{3883B893-216F-4094-AD9A-61...	ITipProperties	0022BAD4	6F8ED018
{8241DDBA-CFA9-42E3-9D7B-4...	ITextCorrectionSite	0022BEC4	6F8ED254
{CC3E4D95-23DD-4C46-8EC4-2...	ITipWindow	0022BA8C	6F8ED030

Looking for functions of Local Server

Object: CLSID_JITDebuggingHost

IID	Name	Addr Interf...	Addr VTable
{00000000-0000-0000-C000-000...	IUnknown	02C23F60	775381F4
{00000020-0000-0000-C000-000...	IMultiQI	02C23F60	775381F4
{0000013D-0000-0000-C000-00...	IClientSecurity	02C23F3C	77538258
{42EF9F29-7777-42ED-BA74-94...	IJITDebuggingHost2	0030BEA4	6D5E8A20
{8E4B97F3-BC4A-4213-836F-55...	IJITDebuggingHost100	0030BE5C	6F86D030

Vtable IJITDebuggingHost2

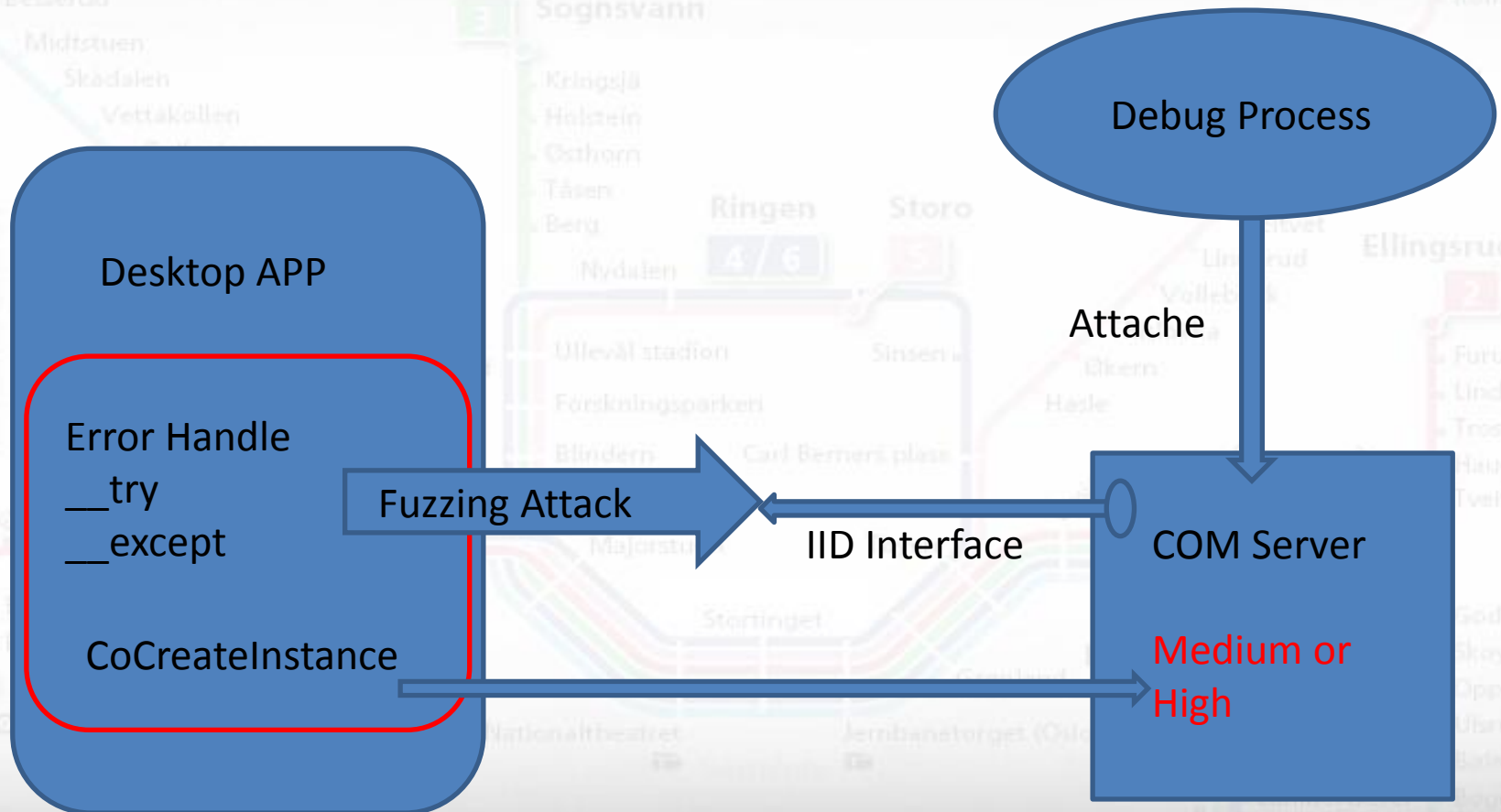
#/Name	Offset	Value
0	0	6D5E2E32
1	4	6D5E2E62
2	8	6D5E2E86
3	12	7760741F

outgoing Interfaces

```

text:00404958 ; const JITDebuggingHost::CHost::`vtable' {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↓
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

WinRT APIs

Communication
& Data

Graphics &
Media

Devices &
Printing

Application Model

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

Background
Transfer

XML

Networking

SMS

Media

Playback

Capture

PlayTo

Visual
Effects

Fundamentals

Application Services

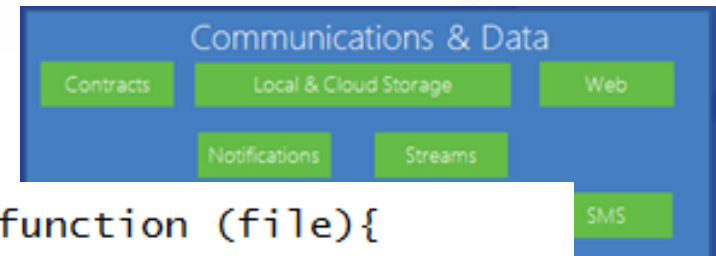
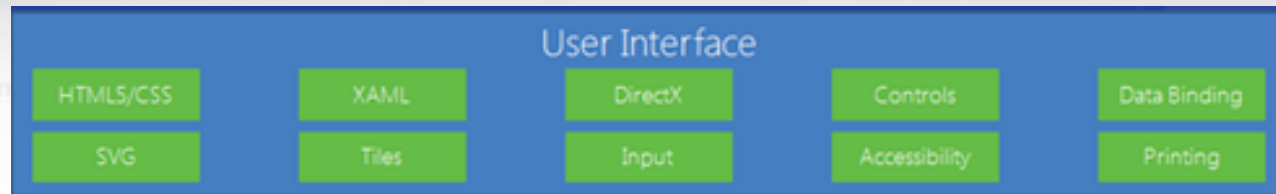
Threading/Timers

Memory Management

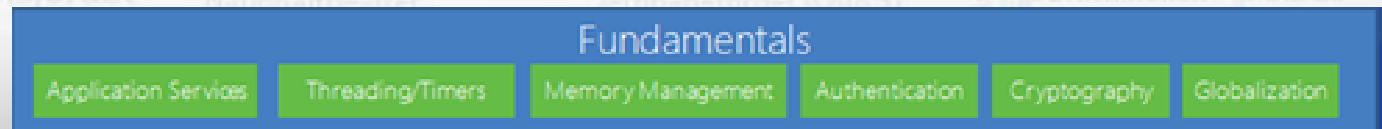
Authentication

Cryptography

Globalization

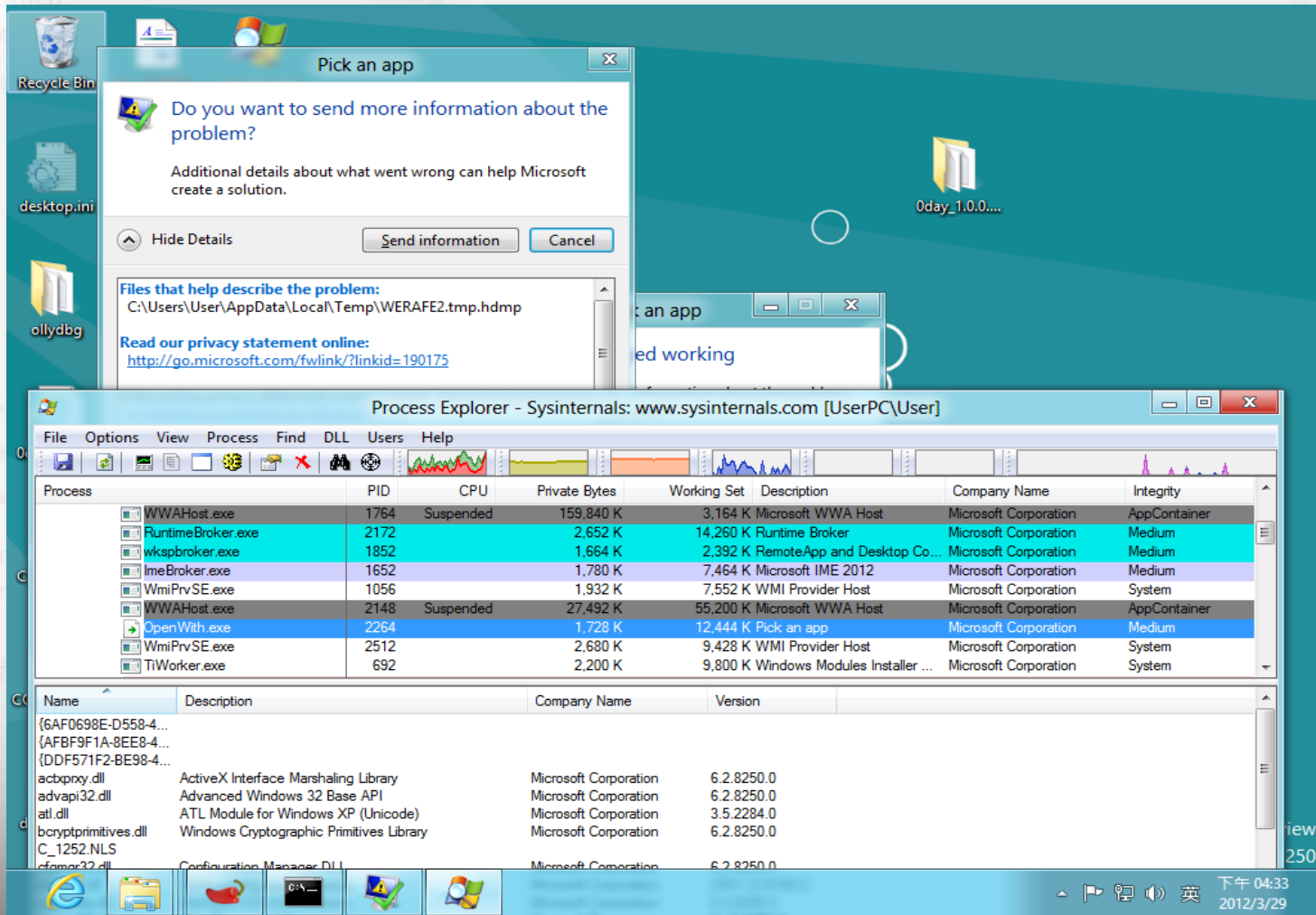


```
savePicker.pickSaveFileAsync().then(function (file){
    if (file) {
        var options = new Windows.System.LauncherOptions();
        options.displayApplicationPicker = true;
        Windows.System.Launcher.launchFileAsync(file, options);
    }
});
```



Discovered an Issue of a Broker Process

- OpenWith.exe (memory corruption)



The screenshot shows a Windows 7 desktop with a blue background. A "Pick an app" dialog box is open, asking "Do you want to send more information about the problem?" with buttons for "Hide Details", "Send information", and "Cancel". Below the buttons, it says "Files that help describe the problem: C:\Users\User\AppData\Local\Temp\WERAFE2.tmp.hdump" and provides a link to Microsoft's privacy statement.

In the background, the Process Explorer window is open, showing a list of processes. The "OpenWith.exe" process is highlighted in blue. Below the process list, the DLLs loaded by the selected process are shown.

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name	Integrity
WWAHost.exe	1764	Suspended	159,840 K	3,164 K	Microsoft WWA Host	Microsoft Corporation	AppContainer
RuntimeBroker.exe	2172		2,652 K	14,260 K	Runtime Broker	Microsoft Corporation	Medium
Wksbroker.exe	1852		1,664 K	2,392 K	RemoteApp and Desktop Co...	Microsoft Corporation	Medium
ImeBroker.exe	1652		1,780 K	7,464 K	Microsoft IME 2012	Microsoft Corporation	Medium
WmiPrvSE.exe	1056		1,932 K	7,552 K	WMI Provider Host	Microsoft Corporation	System
WWAHost.exe	2148	Suspended	27,492 K	55,200 K	Microsoft WWA Host	Microsoft Corporation	AppContainer
OpenWith.exe	2264		1,728 K	12,444 K	Pick an app	Microsoft Corporation	Medium
WmiPrvSE.exe	2512		2,680 K	9,428 K	WMI Provider Host	Microsoft Corporation	System
TiWorker.exe	692		2,200 K	9,800 K	Windows Modules Installer ...	Microsoft Corporation	System

Name	Description	Company Name	Version
{6AF0698E-D558-4...			
{AFBF9F1A-8EE8-4...			
{DDF571F2-BE98-4...			
actxprxy.dll	ActiveX Interface Marshaling Library	Microsoft Corporation	6.2.8250.0
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	6.2.8250.0
atl.dll	ATL Module for Windows XP (Unicode)	Microsoft Corporation	3.5.2284.0
bcryptprimitives.dll	Windows Cryptographic Primitives Library	Microsoft Corporation	6.2.8250.0
C_1252.NLS			
cfmapi.dll	Configuration Manager DLL	Microsoft Corporation	6.2.8250.0

The taskbar at the bottom shows the Start button, Internet Explorer, File Explorer, and several application icons. The system tray on the right shows the date and time: 下午 04:33 2012/3/29.

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

70b35b74 push eax

70b35b75 push eax

Tainted Input Operands: eax

70b35b76 call dword ptr [ecx+18h]

Tainted Input Operands: ecx, StackContents

Faulting Instruction

Basic Block:

70b35b6e mov ecx,

Tainted Input

70b35b70 lea edi,

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 twinvui\CIInmersiveOp

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

ATTACK DESIGN LOGIC



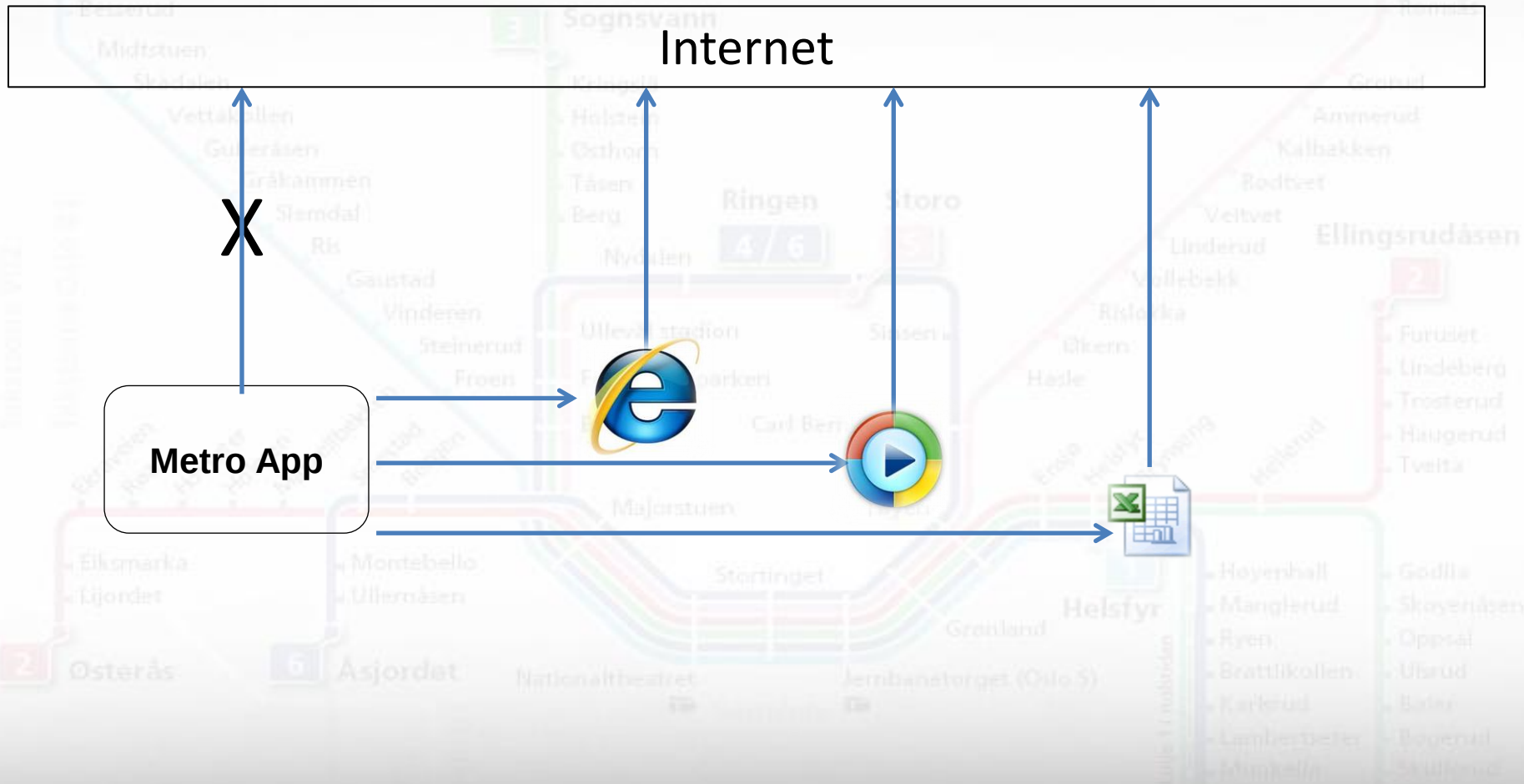
BYPASS INTERNET CONNECTION

FAIL



failblog.org

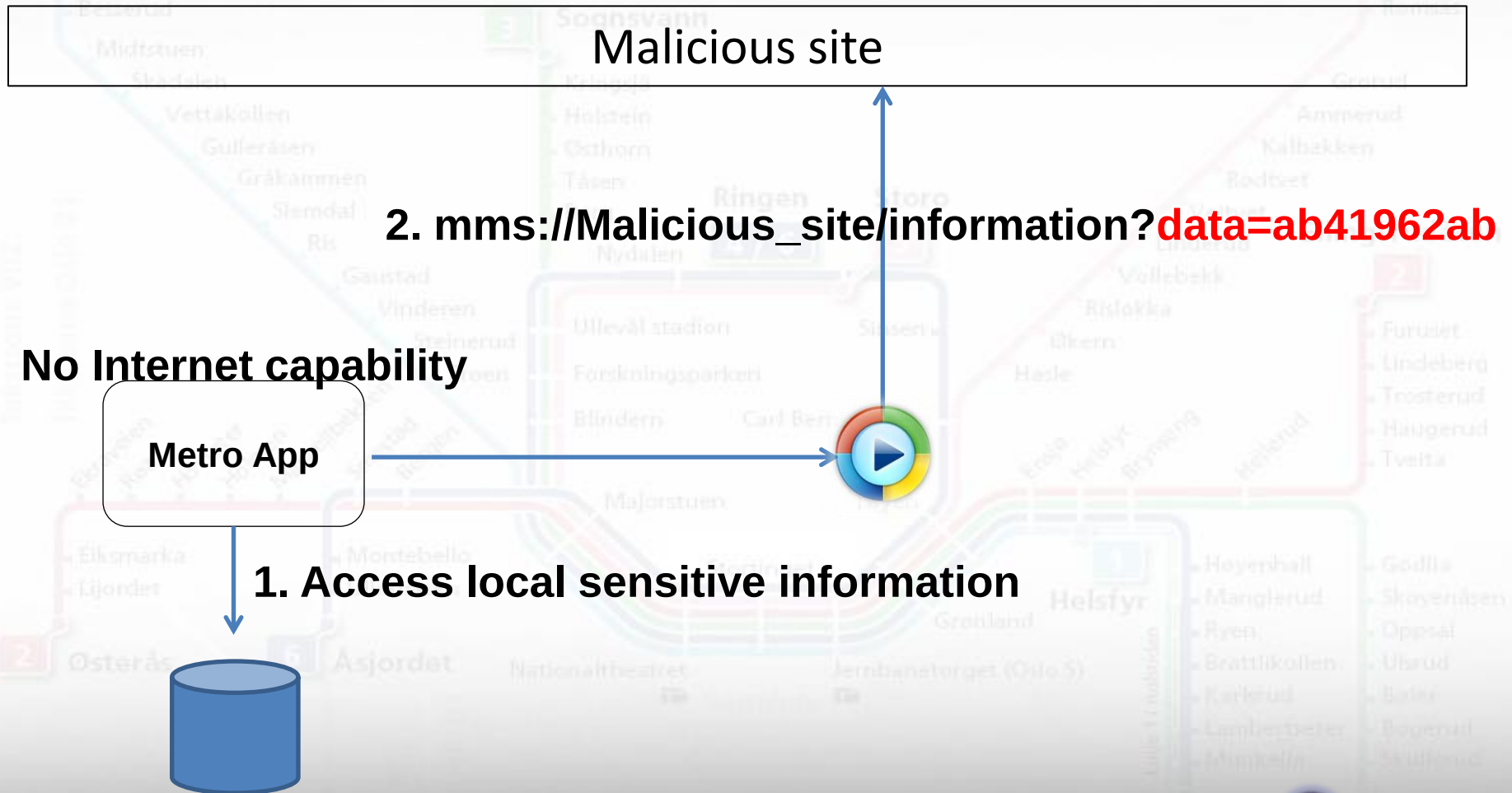
Bypass Internet Connection Limitation



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.

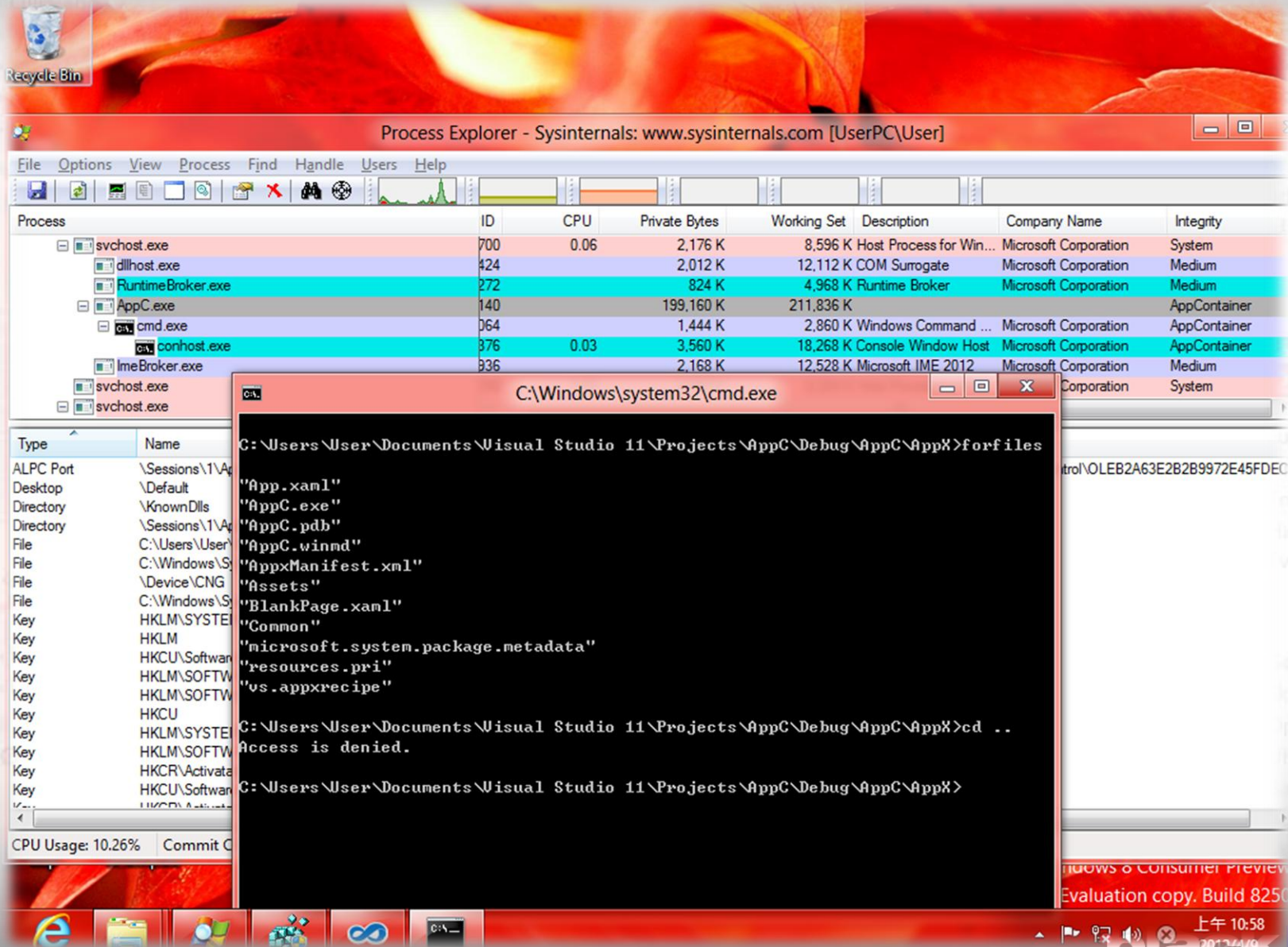
Bypass Internet Connection Limitation



BYPASS LAUNCH PROGRAM LIMITATION



Inline ASM and Shellcode



The screenshot shows a Windows 8 desktop with a red background. A Recycle Bin icon is visible in the top-left corner. The taskbar at the bottom contains icons for Internet Explorer, File Explorer, and other applications. The system clock in the bottom-right corner shows the date 7/28/2012 and time 上午 10:58.

Open windows include:

- Process Explorer - Sysinternals: www.sysinternals.com [UserPC\User]**

Process	ID	CPU	Private Bytes	Working Set	Description	Company Name	Integrity
svchost.exe	700	0.06	2,176 K	8,596 K	Host Process for Win...	Microsoft Corporation	System
dllhost.exe	424		2,012 K	12,112 K	COM Surrogate	Microsoft Corporation	Medium
RuntimeBroker.exe	272		824 K	4,968 K	Runtime Broker	Microsoft Corporation	Medium
AppC.exe	140		199,160 K	211,836 K			AppContainer
cmd.exe	664		1,444 K	2,860 K	Windows Command ...	Microsoft Corporation	AppContainer
conhost.exe	876	0.03	3,560 K	18,268 K	Console Window Host	Microsoft Corporation	AppContainer
imeBroker.exe	836		2,168 K	12,528 K	Microsoft IME 2012	Microsoft Corporation	Medium
svchost.exe							System
- C:\Windows\system32\cmd.exe**

```

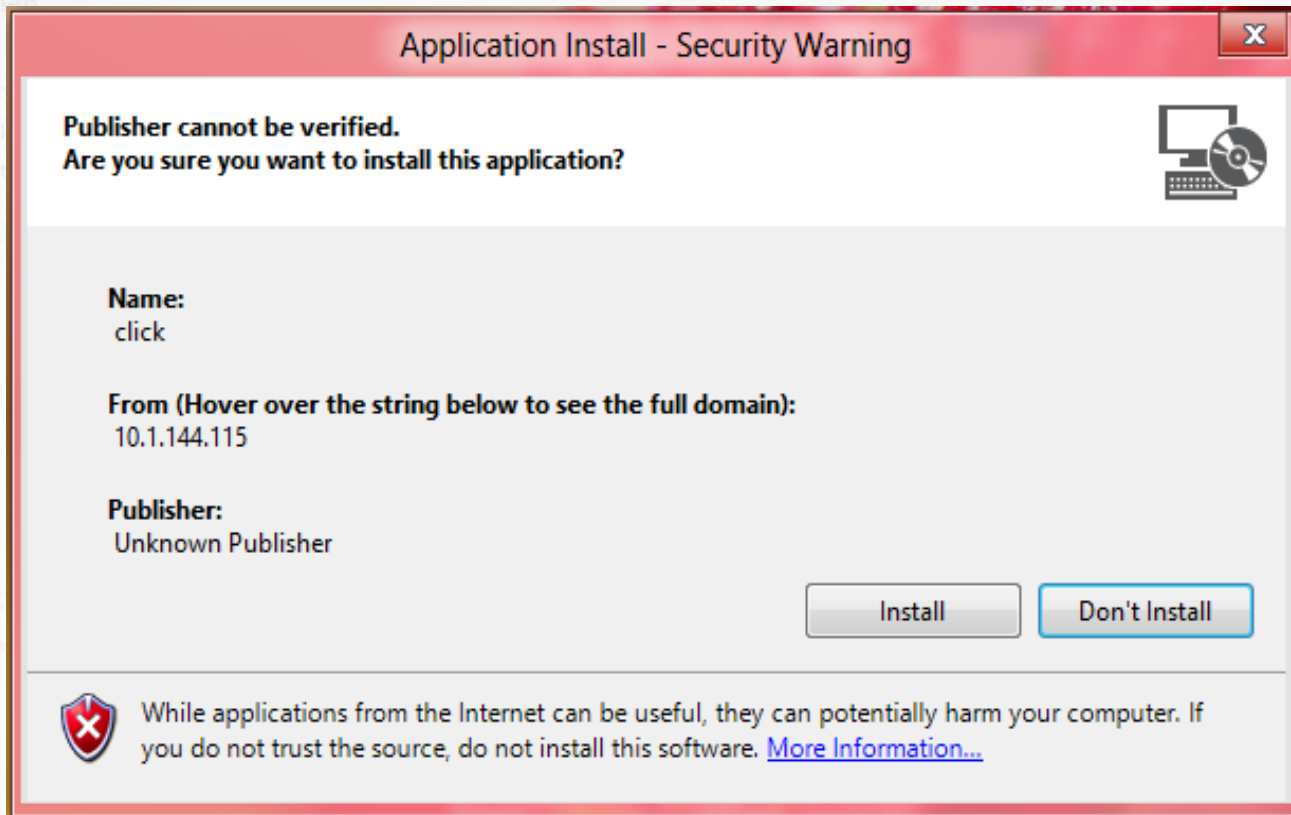
C:\Users\User\Documents\Visual Studio 11\Projects\AppC\Debug\AppC\AppX>forfiles
"App.xaml"
"AppC.exe"
"AppC.pdb"
"AppC.winmd"
"AppxManifest.xml"
"Assets"
"BlankPage.xaml"
"Common"
"microsoft.system.package.metadata"
"resources.pri"
"us.appxrecipe"

C:\Users\User\Documents\Visual Studio 11\Projects\AppC\Debug\AppC\AppX>cd ..
Access is denied.

C:\Users\User\Documents\Visual Studio 11\Projects\AppC\Debug\AppC\AppX>

```

ClickOnce package (.Application/.xbap) is executable



DLL Hijacking

Process Explorer - Sysinternals: www.sysinternals.com [Win8\User]

File Options View Process Find DLL Users Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name	Integrity
vmtoolsd.exe	3156	Suspended	15,432 K	14,180 K	VMware Tools Core Service	VMware, Inc.	Medium
regedit.exe	3424		15,168 K	14,540 K	Registry Editor	Microsoft Corporation	High
oleview.exe	4084		18,400 K	12,376 K	OLE/COM Object Viewer	Microsoft Corporation	Medium
cmd.exe	5420		1,624 K	2,652 K	Windows Command Processor	Microsoft Corporation	High
conhost.exe	5428		1,072 K	6,788 K	Console Window Host	Microsoft Corporation	High
procexp.exe	5004	3.57	191,172 K	214,320 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...	High
COMRaider.exe	4148	< 0.01	13,324 K	18,664 K		iDefense.com	High
notepad.exe	4212		1,248 K	8,284 K	Notepad	Microsoft Corporation	Medium
devenv.exe	2536	1.47	195,912 K	413,904 K	Microsoft Visual Studio 2012 ...	Microsoft Corporation	Medium
Microsoft.VisualStudio.Pe...	4260		24,916 K	36,524 K	Microsoft.VisualStudio.PerfW...	Microsoft Corporation	Medium
conhost.exe	3800		648 K	4,288 K	Console Window Host	Microsoft Corporation	Medium
MSBuild.exe	1176		20,644 K	38,356 K	MSBuild.exe	Microsoft Corporation	Medium
conhost.exe	32		648 K	4,284 K	Console Window Host	Microsoft Corporation	Medium
mmc.exe	220	0.29	29,024 K	12,612 K	Microsoft Management Cons...	Microsoft Corporation	High
explore.exe	5256		4,704 K	17,100 K	Internet Explorer	Microsoft Corporation	Medium
explore.exe	5324		876 K	5,312 K	Internet Explorer	Microsoft Corporation	Low

Name	Description	Company Name	Version	Path
R000000000000006.clb				C:\Windows\Registration\R000000000000006.clb
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\rpcrt4.dll
rsaenh.dll	Microsoft Enhanced Cryptographic...	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\rsaenh.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup ...	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\sechost.dll
secur32.dll	Security Support Provider Interface	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\secur32.dll
setupapi.dll	Windows Setup API	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\setupapi.dll
SHCore.dll	SHCORE	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\SHCore.dll
shell32.dll	Windows Shell Common DLL	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\shell32.dll
shlwapi.dll	Shell Light-weight Utility Library	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\shlwapi.dll
SortDefault.nls				C:\Windows\Globalization\Sorting\SortDefault.nls
sqmapi.dll	SQM Client	Microsoft Corporation	6.2.8400.0	C:\Program Files\Internet Explorer\sqmapi.dll
sspicli.dll	Security Support Provider Interface	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\sspicli.dll
traceextn.dll				C:\Users\User\Desktop\traceextn.dll
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	10.0.8400.0	C:\Windows\System32?urlmon.dll
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\user32.dll
uxtheme.dll	Microsoft UxTheme Library	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\uxtheme.dll
winhttp.dll	Windows HTTP Services	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\winhttp.dll
wininet.dll	Internet Extensions for Win32	Microsoft Corporation	10.0.8400.0	C:\Windows\System32\wininet.dll
winnsi.dll	Network Store Information RPC int...	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\winnsi.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	6.2.8400.0	C:\Windows\System32\ws2_32.dll

CPU Usage: 8.82% Commit Charge: 36.07% Processes: 62 Physical Usage: 56.94%

7/28/2012 8:06 AM 6/20/2012

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