

ANDY FREEBORN

NEBRASKA CYBER SECURITY CONFERENCE 2017

INTRO TO WINDOWS COM

AGENDA

- ▶ What's this Windows COM thing?
- ▶ COM background
- ▶ COM exploitation
- ▶ Demos along the way

LULZ, LET'S STARE AT C++ INSTEAD

```
typedef struct IPersistVtbl
{
    HRESULT ( STDMETHODCALLTYPE *QueryInterface )(
        IPersist * This,
        /* [in] */ REFIID riid,
        /* [iid_is][out] */ void **ppvObject);

    ULONG ( STDMETHODCALLTYPE *AddRef )(
        IPersist * This);

    ULONG ( STDMETHODCALLTYPE *Release )(
        IPersist * This);

    HRESULT ( STDMETHODCALLTYPE *GetClassID )(
        IPersist * This,
        /* [out] */ CLSID *pClassID);
} IPersistVtbl;

struct IPersist
{
    const struct IPersistVtbl *lpVtbl;
};
```

WHAT'S THIS WINDOWS COM THING?

- ▶ Stands for “Component Object Model”
- ▶ Designed in the 90s to be interoperable, portable
 - ▶ It's old; great books aren't digital
- ▶ Not a “Shell” like CMD or PowerShell
- ▶ “Like” .NET and WMI
- ▶ Why am I so interested in this?

GET PRINT BOOK

No eBook available

Addison-Wesley Professional

Amazon.com

Barnes&Noble.com - \$31.49 and up

Books-A-Million

IndieBound

Find in a library

All sellers »



G+



7 Reviews

Write review

Essential COM

By Don Box

WHAT'S THIS WINDOWS COM THING? RULE #1: WE DON'T SPEAK ABOUT COM

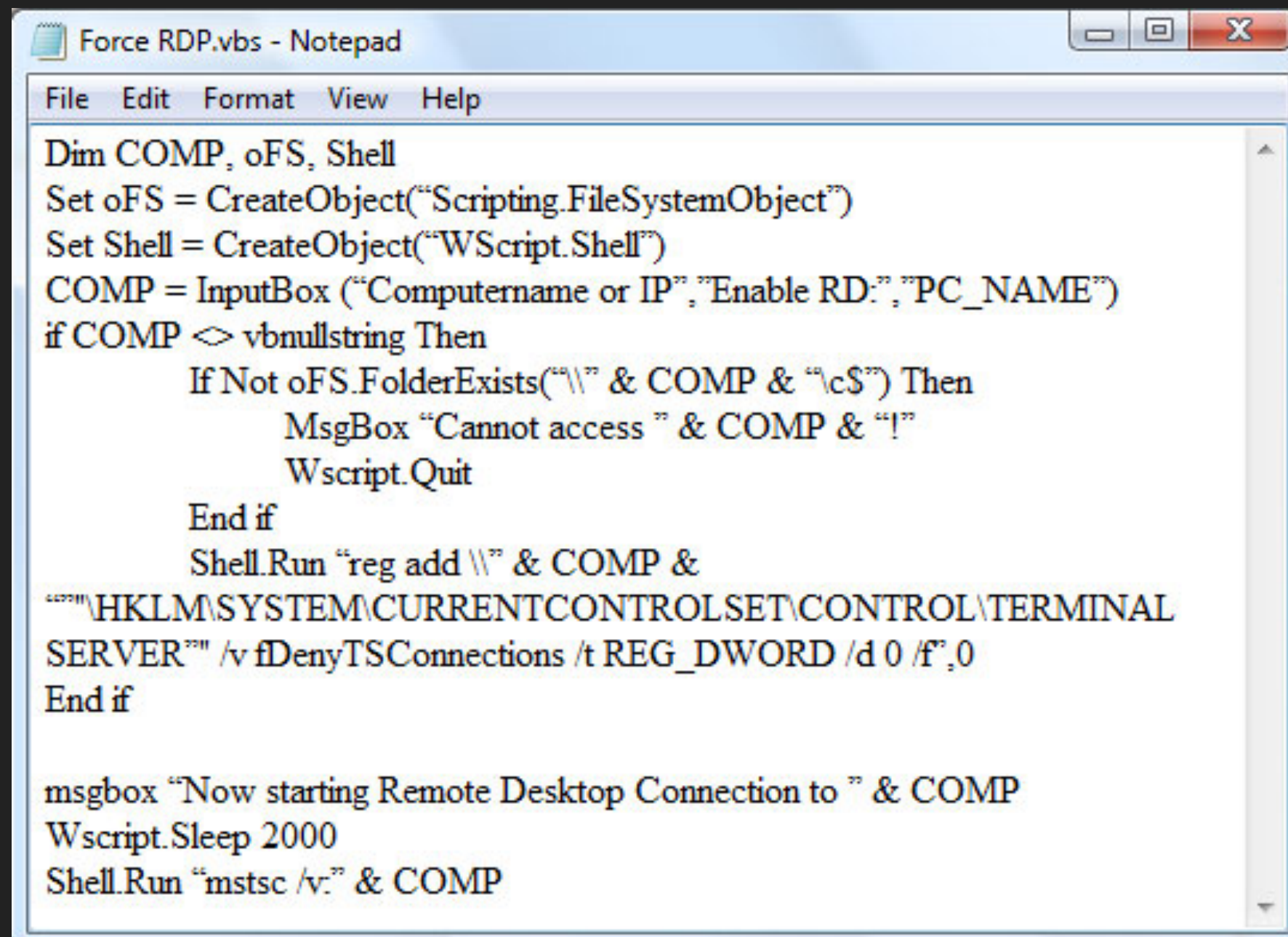
- ▶ Used everywhere in Windows
 - ▶ When a user copies files, embeds Excel within Word
- ▶ It's abstracted away with GUIs, .Net, APIs, and hardly anyone acknowledges (or knows!) COM was used



- ▶ Obligatory COM history
 - ▶ Precursor to .NET
 - ▶ Meant to solve problems with developers like DLLs
- ▶ There's so many COM objects and won't go away
- ▶ OLE and ActiveX fit in here
 - ▶ OLE (Object Linking and Embedding) lets you embed things (e.g. Excel sheet inside Word)
 - ▶ ActiveX lets Internet Explorer make bad life choices

COM BACKGROUND: COM ON PAPER IS SUPER EASY TO WORK WITH

- ▶ Access COM things thru interfaces and objects
 - ▶ Scripting.FileSystemObject
 - ▶ IPersist
 - ▶ IFileOperation
 - ▶ WScript.Shell



```
Force RDP.vbs - Notepad
File Edit Format View Help

Dim COMP, oFS, Shell
Set oFS = CreateObject("Scripting.FileSystemObject")
Set Shell = CreateObject("WScript.Shell")
COMP = InputBox ("Computername or IP", "Enable RD:", "PC_NAME")
if COMP <> vbnullstring Then
    If Not oFS.FolderExists("\\ " & COMP & "\c$") Then
        MsgBox "Cannot access " & COMP & "!"
        Wscript.Quit
    End if
    Shell.Run "reg add \\ " & COMP &
"""\HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL
SERVER"" /v fDenyTSConnections /t REG_DWORD /d 0 /f",0
End if

msgbox "Now starting Remote Desktop Connection to " & COMP
Wscript.Sleep 2000
Shell.Run "mstsc /v:" & COMP
```

COM BACKGROUND: COM MAKES YOU WORK FOR IT

► COM is a hot mess

Windows PowerShell

```
PS C:\Users\IEUser> $com = New-Object -ComObject WScript.Shell
PS C:\Users\IEUser> $com
```

SpecialFolders	CurrentDirectory
-----	-----
System.__ComObject	C:\Users\IEUser

```
PS C:\Users\IEUser> $com | Get-Member
```

TypeName: System.__ComObject#{41904400-be18-11d3-a28b-00104bd35090}

Name	MemberType	Definition
----	-----	-----
AppActivate	Method	bool AppActivate (Variant, Va
CreateShortcut	Method	IDispatch CreateShortcut (str
Exec	Method	IWshExec Exec (string)
ExpandEnvironmentStrings	Method	string ExpandEnvironmentStrin
LogEvent	Method	bool LogEvent (Variant, strin
Popup	Method	int Popup (string, Variant, V
RegDelete	Method	void RegDelete (string)
RegRead	Method	Variant RegRead (string)
RegWrite	Method	void RegWrite (string, Varian
Run	Method	int Run (string, Variant, Var
SendKeys	Method	void SendKeys (string, Varian
Environment	ParameterizedProperty	IWshEnvironment Environment (
CurrentDirectory	Property	string CurrentDirectory () {g
SpecialFolders	Property	IWshCollection SpecialFolders

COM BACKGROUND: ITS LIKE COM MAKES UP THE RULES AS IT GOES ALONG

- ▶ No, COM really is a hot mess and can live in:

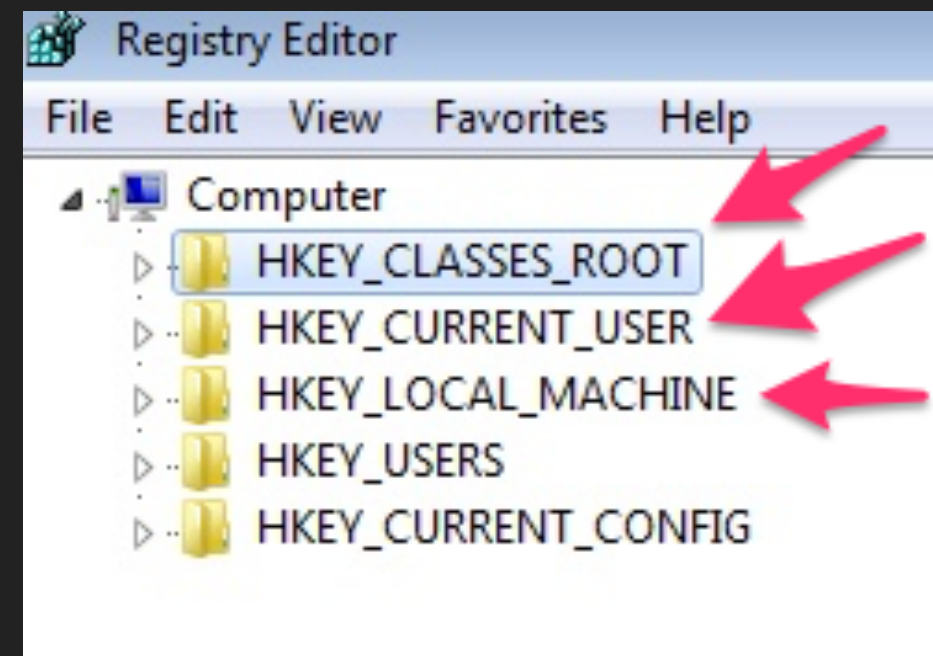
- ▶ Windows Registry

- ▶ Windows made a special registry hive

- ▶ HKCR (HKEY_Classes_Root)

- ▶ Combines HKLM and HKCU

- ▶ Threading / InProcServer32



- ▶ Manifest files (COM scriptlets; Registration free too!)

COM BACKGROUND: COM MAKES YOU WORK FOR IT

▶ WScript.Shell demo

```
Windows PowerShell
PS C:\Users\IEUser> $com = New-Object -ComObject WScript.Shell
PS C:\Users\IEUser> $com

SpecialFolders                                CurrentDirectory
-----
System.__ComObject                            C:\Users\IEUser

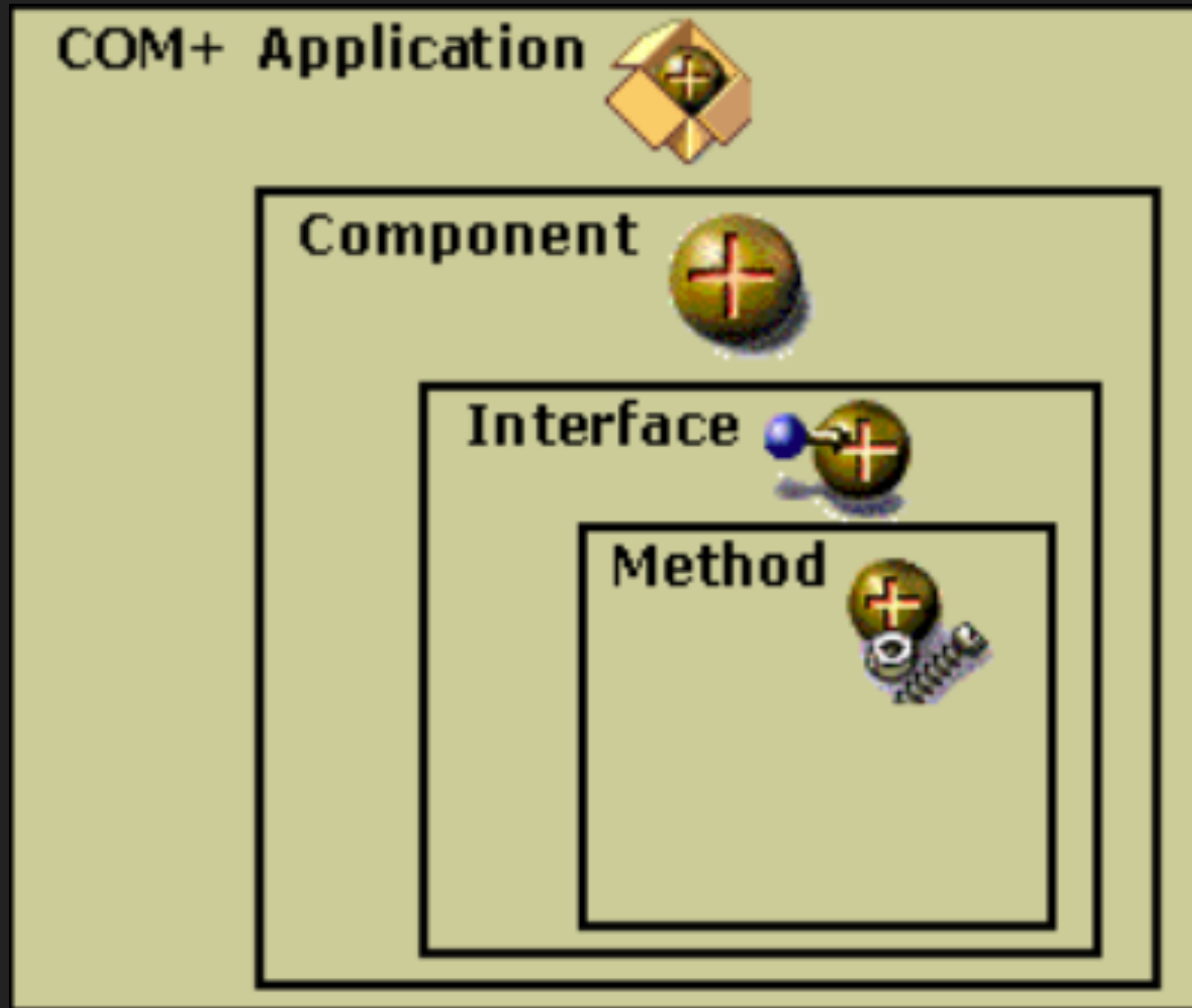
PS C:\Users\IEUser> $com | Get-Member

TypeName: System.__ComObject
Interface ID: {41904400-be18-11d3-a28b-00104bd35090}

Name      MemberType      Definition
----      -
AppActivate Method          bool AppActivate (Variant, Variant)
CreateShortcut Method         IDispatch CreateShortcut (string, string)
Exec      Method          IWshExec Exec (string)
ExpandEnvironmentStrings Method         string ExpandEnvironmentStrings (string)
LogEvent  Method          bool LogEvent (Variant, string)
Popup    Method          int Popup (string, Variant, Variant)
RegDelete Method          void RegDelete (string)
RegRead   Method          Variant RegRead (string)
RegWrite  Method          void RegWrite (string, Variant)
Run       Method          int Run (string, Variant, Variant)
SendKeys  Method          void SendKeys (string, Variant)
Environment ParameterizedProperty IWshEnvironment Environment (Variant)
CurrentDirectory Property         string CurrentDirectory () {get}
SpecialFolders Property         IWshCollection SpecialFolders
```

- ▶ COM+ meant to solve the problems in COM like:
 - ▶ Quickly implement common configurations for COM components like security boundaries
 - ▶ Load DLLs into processes on demand
 - ▶ Managed methods to manage COM components
 - ▶ Multi-pass... err.. threading
 - ▶ Slick GUI

- ▶ COM+ also came with rad icons in the GUI
- ▶ Demo!



ZeroSum tweeted about a COM+ scriptlet, but how would you know it's COM+ and not COM?

 **zerosum0x0** 
@zerosum0x0

Following

Not "completely fileless", COM+ scriptlets will be written to
%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\



Binni Shah @binitamshah

A Look at JS_POWMET - a Completely Fileless Malware :
blog.trendmicro.com/trendlabs-secu ...

10:39 PM - 5 Aug 2017

- ▶ Scriptlets come in both COM and COM+ flavors
- ▶ They allow you to have COM scripts to do non-malicious things like open calculator and cmd shells
- ▶ Did you know you can create COM objects from a Java class? Good thing no one has a JRE installed.

Creating an Object from a Java Class

To use `Server.CreateObject` to create an instance of a Java class, you must use the JavaReg program to register the class as a COM component. You can then use `Server.CreateObject` method or an HTML `<OBJECT>` tag with the PROGID or CLSID.

Alternatively, you can use the mechanism provided by Java monikers to instantiate the Java class directly without using the JavaReg program. To instantiate a class with monikers, use the VBScript or JScript `GetObject` statement and provide the full name of the Java class in the form

`java:classname`

HAX: REGSVR32 /S /N /U /I:BACKDOOR-MINIMALIST.SCT SCROBJ.DLL

- ▶ subTee example: COM manifest file
- ▶ Demo!

 Backdoor-Minimalist.sct

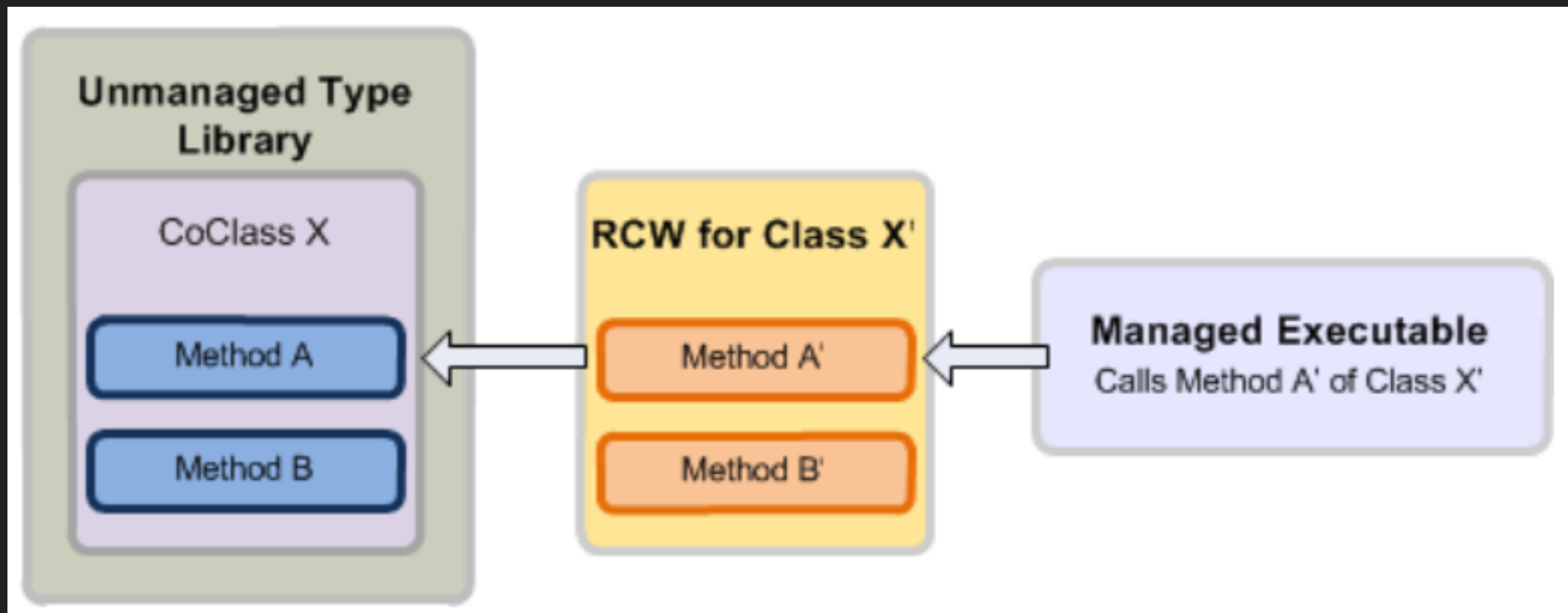
```
1  <?XML version="1.0"?>
2  <scriptlet>
3  <registration
4      progid="PoC"
5      classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
6          <!-- Proof Of Concept - Casey Smith @subTee -->
7          <!-- License: BSD3-Clause -->
8          <script language="JScript">
9              <![CDATA[
10
11                  var r = new ActiveXObject("WScript.Shell").Run("calc.exe");
12
13              ]]>
14      </script>
15  </registration>
16  </scriptlet>
```

<https://gist.github.com/subTee/24c7d8e1ff0f5602092f58cbb3f7d302>

- ▶ regsvr32 is used to register many things in the registry
 - ▶ /s runs it silently, /n says to not call DllRegisterServer
 - ▶ /u specifies which COM server to uninstall
 - ▶ /i calls DllInstall for the COM object and cmd options
 - ▶ Can be pointed to a file on your system
 - ▶ Can be a URL (http: COM moniker)
 - ▶ Could even be a Java class (java: COM moniker)
- ▶ scrobj.dll makes the magic go

- ▶ DCOM is “Distributed COM”
 - ▶ “Helps you” in COM and COM+ with distributed transactions
 - ▶ Slings COM object data typically with RPC
 - ▶ Likes to make assumptions you know what you’re doing with security and marshaling data
 - ▶ James Forshaw and Matt Nelson have been finding problems with Windows and apps marshaling data

- ▶ .NET can work with COM for interoperability
 - ▶ “The Runtime Callable Wrapper (RCW) is a mechanism that promotes transparent communication between COM and the managed programming model.”



COM BACKGROUND: BREAKING DOWN THAT SWEET RCW GOODNESS

- ▶ This is what PowerShell uses to call into COM objects
 - ▶ System.Management.Automation is a huge library

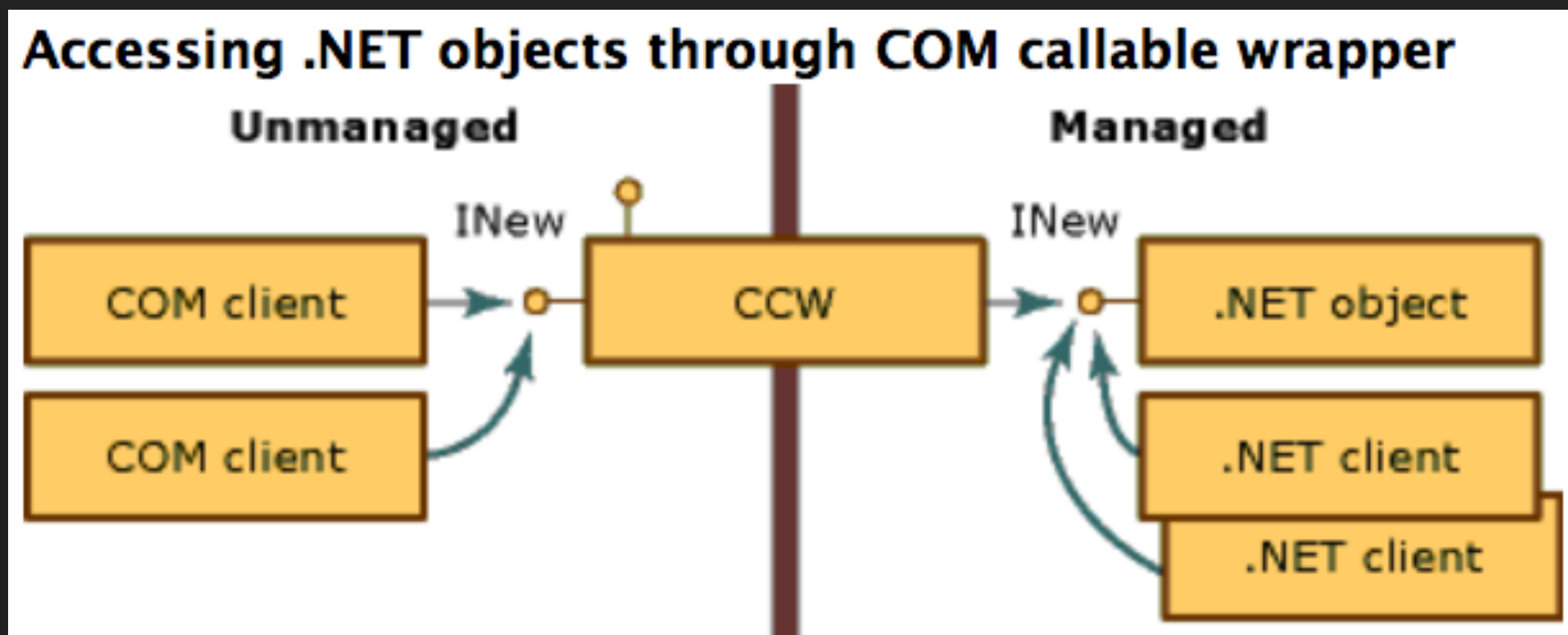
```
namespace System.Management.Automation.ComInterop
{
    /// <summary>
    /// This is a helper class for runtime-callable-wrappers of COM instances. We create one instance of this type
    /// for every generic RCW instance.
    /// </summary>
    internal class ComObject : IDynamicMetaObjectProvider
    {
        internal ComObject(object rcw)
        {
            Debug.Assert(ComObject.IsComObject(rcw));
            RuntimeCallableWrapper = rcw;
        }

        /// <summary>
        /// The runtime-callable wrapper
        /// </summary>
        internal object RuntimeCallableWrapper { get; }

        private static readonly object s_comObjectInfoKey = new object();
    }
}
```

<https://github.com/PowerShell/PowerShell/blob/master/src/System.Management.Automation/engine/ComInterop/ComObject.cs>

- ▶ COM can work with .Net thru COM Callable Wrappers
- ▶ “When a COM client calls a .NET object, the common language runtime creates the managed object and a COM callable wrapper (CCW) for the object. Unable to reference a .NET object directly, COM clients use the CCW as a proxy for the managed object.”



COM BACKGROUND: DEEP TECHNICAL DETAIL OF THAT MAGIC

- ▶ James Forshaw talked about .Net and COM interoperability last Saturday at DerbyCon
- ▶ IronGeek Link: ig2.me/pZ


The .NET Inter-Operability Operation
James Forshaw
Derbycon 2017

...y to call native code, whether that's APIs exposed from dynamic libraries or remote COM objects. Adding this in-built functionality to an "type-safe" runtime has
...NET runtime implements its various Interop features, where the bodies are buried and how to use that to find issues ranging from novel code execution mecha
...presentation will assume the attendee has some familiarity with .NET and how the runtime executes code.

...s been involved with computer hardware and software security for over 10 years looking at a range of different platforms and applications. With a great interest
...he breakouts as well as being a Pwn2Own and Microsoft Mitigation Bypass bounty winner. He has spoken at a number of security conferences including Black

[@tiranidra](#)

S12 The .NET Inter Operability Operation James Forshaw

Let's Interop  te!



- ▶ Eventually, you're going to have to deal with C, C++

```
typedef struct IPersistVtbl
{
    HRESULT ( STDMETHODCALLTYPE *QueryInterface )(
        IPersist * This,
        /* [in] */ REFIID riid,
        /* [iid_is][out] */ void **ppvObject);

    ULONG ( STDMETHODCALLTYPE *AddRef )(
        IPersist * This);

    ULONG ( STDMETHODCALLTYPE *Release )(
        IPersist * This);

    HRESULT ( STDMETHODCALLTYPE *GetClassID )(
        IPersist * This,
        /* [out] */ CLSID *pClassID);
} IPersistVtbl;

struct IPersist
{
    const struct IPersistVtbl *lpVtbl;
};
```

COM EXPLOITATION: THAT WASN'T SO BAD!




- ▶ QueryInterface is how you query... for interfaces
 - ▶ This is how you figure out what interfaces are available to you
- ▶ AddRef / Release may be important to you eventually
 - ▶ Important if you want to partake in bug bounties :)
 - ▶ This dictates the object lifetime by reference count
 - ▶ Abusing the reference count introduces other avenues of attack (cough Use After Free)

COM EXPLOITATION: USE AFTER FREE HAS ALWAYS BEEN AN ISSUE

- ▶ Raymond Chen talked about this in 2004

Reference counting is hard.

 Raymond Chen - MSFT April 6, 2004

<https://blogs.msdn.microsoft.com/oldnewthing/20040406-00/?p=39903>

- ▶ Exploit DB has stuff on AddRef being misused

Mozilla Firefox < 50.1.0 - Use-After-Free

EDB-ID: 41042	Author: Marcin Ressel	Published: 2017-01-13
CVE: CVE-2016-9899	Type: Dos	Platform: Windows
E-DB Verified: 	Exploit:  Download /  View Raw	Vulnerable App: 

```
* eip=6d7cc44c esp=003be0b8 ebp=003be0cc iopl=0
* cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b
* xul!mozilla::net::LoadInfo::AddRef+0x3dd41:
* 6d7cc44c ff12          call     dword ptr [edx]
* 0:000> dd eax
* 0f804c00  4543484f 91919191 91919191 91919191
```

<https://www.exploit-db.com/exploits/41042/>

- ▶ Microsoft has been fixing COM issues for a long time
 - ▶ MS Bulletins will be posted on my website
- ▶ Researched by Haifei Li, Mark Dowd, James Forshaw
 - ▶ Links will be posted on my website
- ▶ We hear about COM at conferences, goes silent, gets "rediscovered", and its still broke (lulz)

COM EXPLOITATION: WHAT ARE FUN WAYS COM HAS BEEN EXPLOITED?

▶ How is COM exploited?

▶ UACMe

5. Author: WinNT/Simda

- Type: Elevated COM interface
- Method: ISecurityEditor
- Target(s): HKLM registry keys

▶ James Forshaw

Wednesday, August 23, 2017

Bypassing VirtualBox Process Hardening on Windows

▶ Casey Smith

Wednesday, April 26, 2017

Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)

▶ Matt Nelson

BYPASSING AMSI VIA COM SERVER HIJACKING

July 19, 2017 by enigma0x3

Microsoft's Antimalware Scan Interface

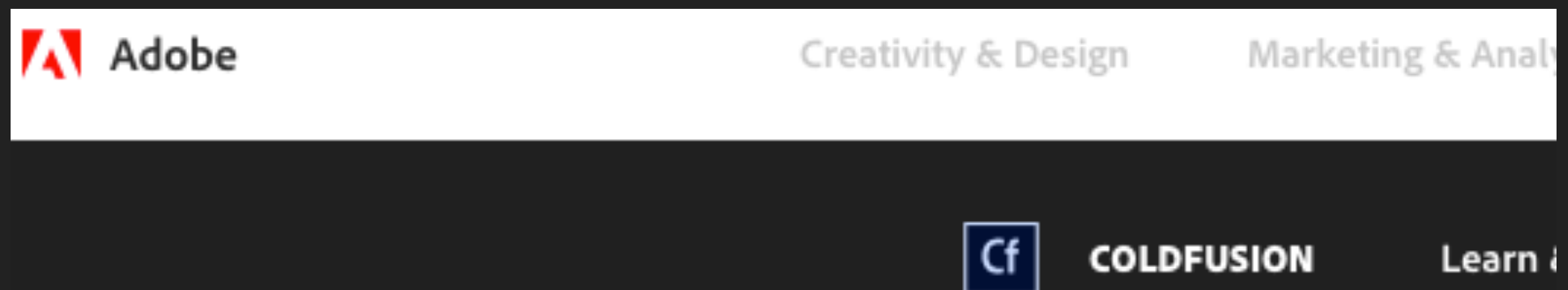
COM EXPLOITATION: WHAT TOOLS CAN I USE TO LEARN MORE? ALL FREE!

- ▶ Microsoft Process Explorer
 - ▶ Helpful to find medium to high integrity exploitation
- ▶ ReactOS
- ▶ James Forshaw OleViewDotNet (github.com/tyranid/oleviewdotnet)
 - ▶ "OleViewDotNet is a .NET 4 application to provide a tool which merges the classic SDK tools OleView and Test Container into one application. It allows you to find COM objects through a number of different views (e.g. by CLSID, by ProgID, by server executable), enumerate interfaces on the object and then create an instance and invoke methods. It also has a basic container to attack ActiveX objects to so you can see the display output while manipulating the data."

ITS ALMOST TIME TO GO, LETS REVIEW QUICKLY

- ▶ COM is everywhere like how we saw today with Thug
- ▶ Not covered: Integrity levels, "TreatAs", and monikers
- ▶ Many "exploits" are just abusing design decisions
- ▶ More research and community made tools will (most likely) bring to light more COM exploits and wreckage
- ▶ Other organizations also add their own COM objects

▶ Adobe:



Creating and using COM objects

WE NEED THE BLUE TEAM, AND THEY NEED US

- ▶ There's a lot of fun new COM focused tools out
 - ▶ ZeroSum, et al released Koadic: COM C&C
- ▶ Casey, SpecterOps, and attackers are focused on COM
- ▶ We need to use their research to our gain
 - ▶ We need to run these tools internally... Squiblydoo
 - ▶ There are ways to reduce the COM attack surface
 - ▶ Work with the product groups and blue team
 - ▶ See how these products trigger IOCs and act