BleedingEdge

笔记本：	ALPC		
创建时间：	2019/7/28 11:24	更新时间：	2019/8/22 10:49
作者：	188aqhwv323		
URL：	https://www.baidu.com/s?wd=%E7%BA%A6%E7%AD%89%E4%BA%8E%E5%8F%B7&rsv_sp…		

****### Intro

Why Sandbox?

JSEngine bug in browser can do few things unless coordinate with a SandboxEscape bug.
From a realworld view,
A SandboxEscape bug's is very valuable.
Which is really hard to find.

Sandbox in CTF

GoogleCTF 2019
Sandbox Part:

4 PWN
3 REVERSING
4 WEB
5 SANDBOX

What's the difficulty about Sandbox?

Highly relying on Operating System Privilege Mechanisms.
Linux: Seccomp, namespace ...
Windows: AppContainer, Integrity level, SACL/DACL...
...

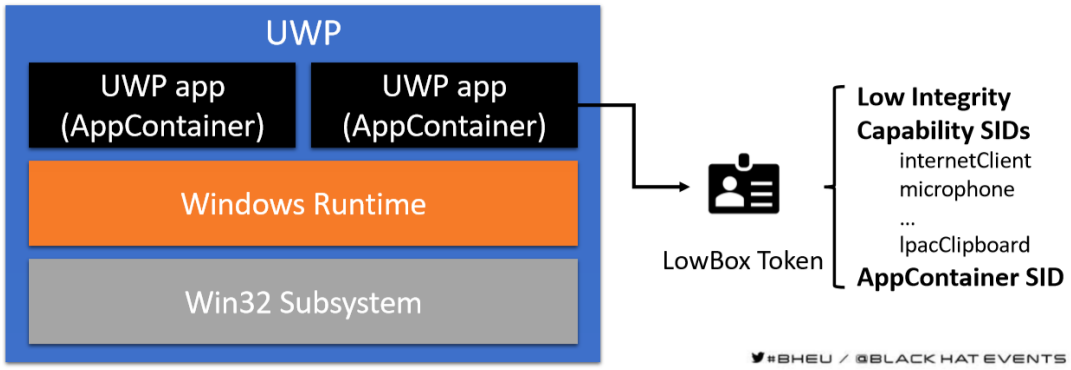
What's in this challenge?

Server.exe:

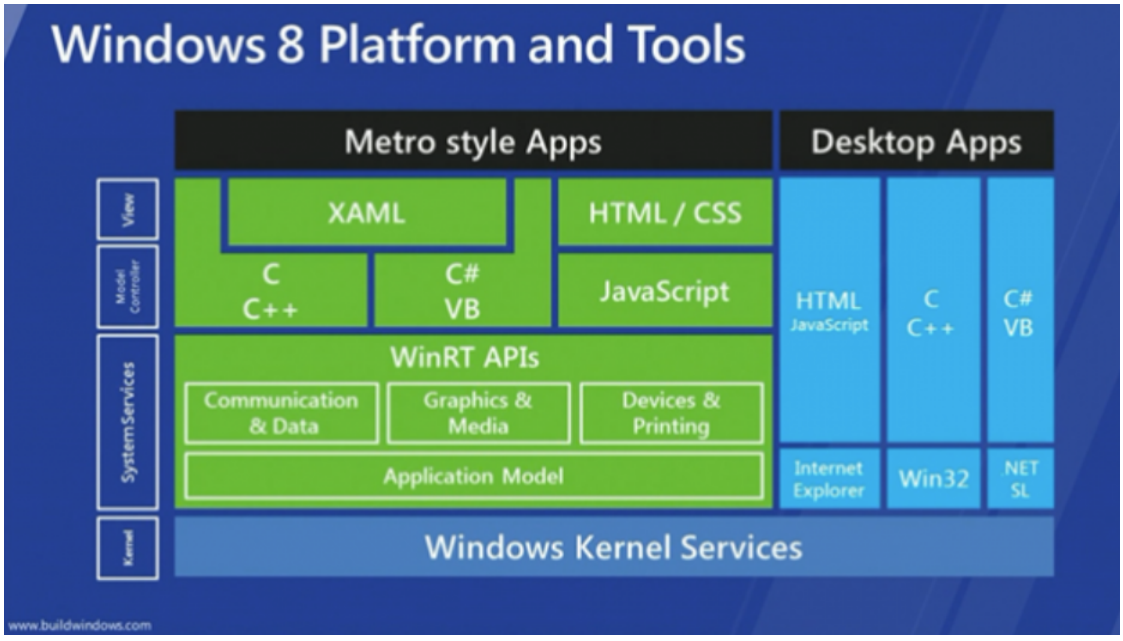
1. Get MicrosoftEdge's ManageAppContainer's privilege token.
2. Create an AppContainer with default privilege
3. Drop a File with arbitrary content under Sandbox{random file name}
4. Impersonate MicrosoftEdge's token and launch any program specified.

What can appcontainer do?

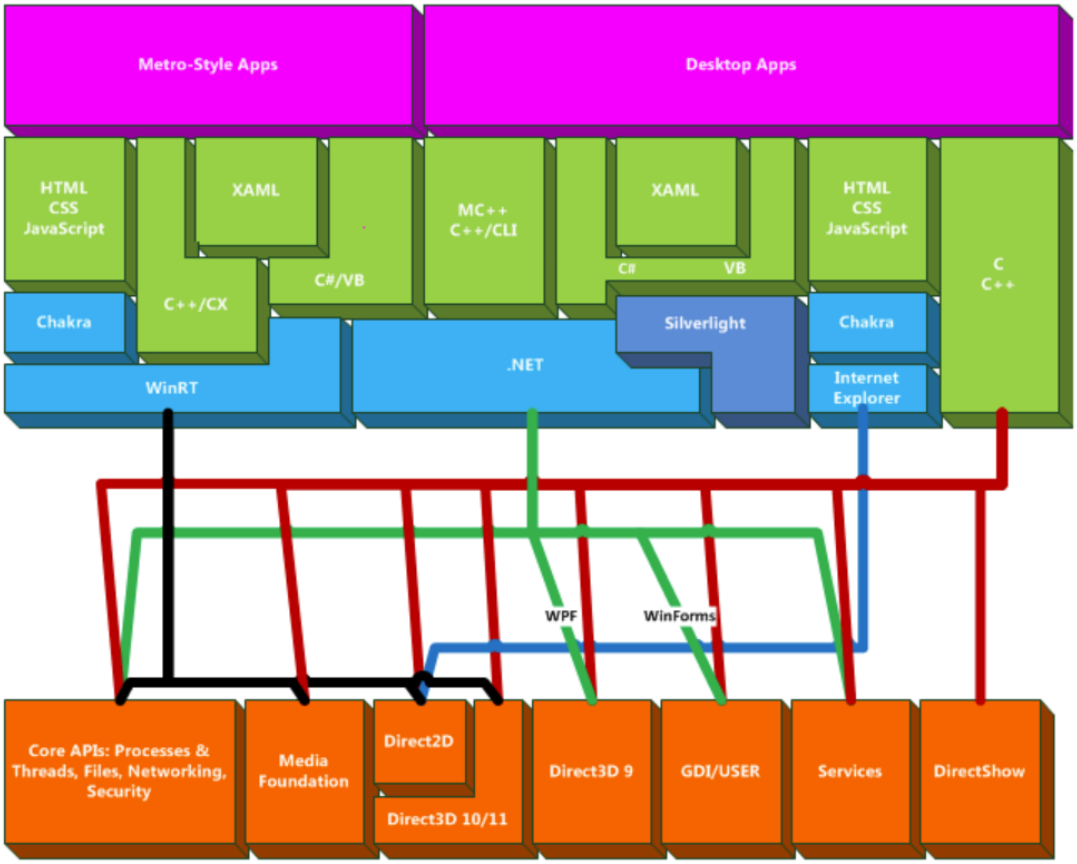
MicrosoftEdge's AppContainer Structure:



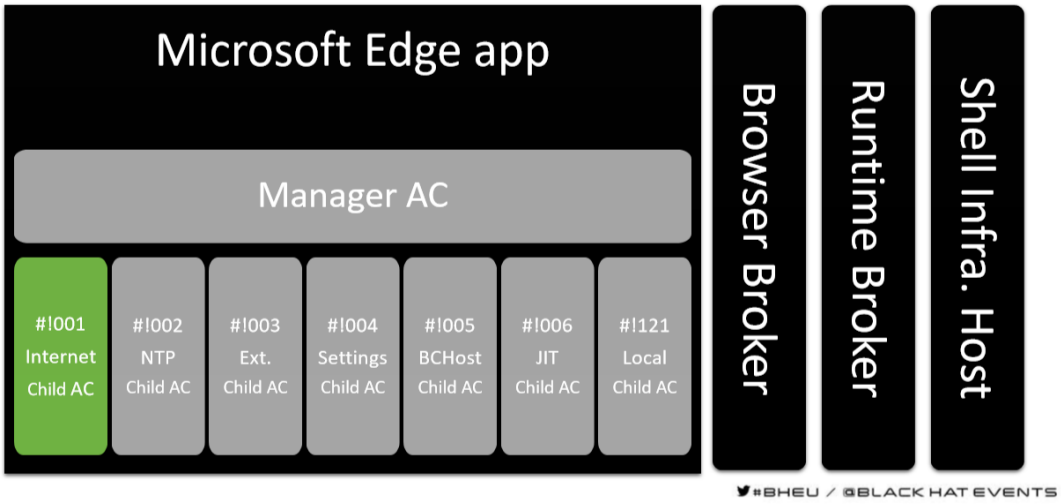
关于WinRT的架构：
曾经微软给出的WinRT架构如下图所示：



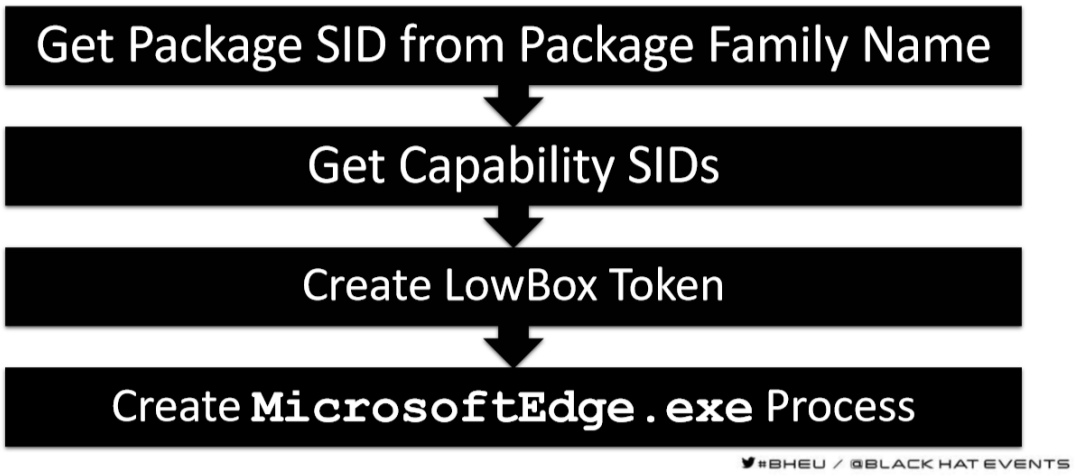
但实际上，真实架构如下图所示：



What about Edge's Container?



EdgeContainer CreateProcedure:



Are there any guards in Edge?

1. ACG(Arbitrary Code Guard)
2. CIG(Code Integrity Guard)
3. Child Process Policy(CreateProcess Banned)
4. JIT Engine Seperation(JIT Process Seperated)

Which means , if you get arbitrary mem R/W, if you want rce as normal user with medium integrity, you need:
(1). Find a way to do RCE.
(2). From ChildAP to ManagerAP
(3). From ManagerAP to normaluser(this challenge in)

AppManager.exe:

Implements a RPCServer with RPCVersion 1.0

```
1. CopyAppFile(void *h1, wchar_t *destpath, wchar_t *srcpath)
2. SetUpApp(void *h1, configer *configops, wchar_t *configfile)
3. RunApp(void *h1, wchar_t *target, configer *configops, runmode *rmode)
```

1 CopyAppFile:
Copy a file from user-specified srcpath to file under:

C:\Users\11236\AppData\Local\Packages\nese.bleedingedge_8wekyb3d8bbwe\AC\Temp

to trigger this RPC:
(1). you must be MicrosoftEdge
(2). srcpath is accessed with ImpersonationClient

2 SetUpApp:

Copy a config file from user-specified srcpath to file under:

C:\Users\11236\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Temp

to trigger this RPC:

(1). **you must not be MicrosoftEdge**
(2). srcpath must under:

C:\Users\11236\AppData\Local\Packages\nese.bleedingedge_8wekyb3d8bbwe\AC\Temp

3 RunApp

(1) Specify a dll to **load**
(2) Check If you are MicrosoftEdge, you can invoke LoadLibrary.

So what you can do with all things above:

(1). Create an AppContainer with default Privilege(which is very low)
(2). Upload an exe or dll or whatever with limited size.
(3). CreateProcess within the Created Appcontainer
(4). CreateProcess with MicrosoftEdge's token
(5). Rpc Reverse and then interact with AppManagerSvc

Exploit

---

(1). CreateAppcontainer A
(2). Upload Signed "calc.exe"
(3). Upload Real Payload
(4). Trigger RPC, move the calc.exe into NeSE's AppContainer Folder
(5). Trigger RPC, move the calc.exe into Edge's AppContainer Folder
(6). Trigger RPC, move Real Payload into Edge's AppContainer Folder and rename it as System DLL's name
(7). Make a Process with MicrosoftEdge's token, let it run "calc.exe" under Edge's AppContainer Folder.
(8). calc.exe load payload **DLL hijack done.**
(9). Payload Then Trigger RPC, Request RPCServer to load an malicious DLL to reverse binding a shell and then read flag under C:\flag.txt.

Question: How to Bypass Microsoft Code Integrity Check with ACG and CIG>

(1). ROP
(2). Load a TRUSTED Image, which will **load** other images without Code Integrity Check, then perform DLL hijack.
(3) Abuse JS Engine to get RCE in JIT Process.(ProjectZero)
