

2019: a local hacking odyssey

The MITM attack against password manager

Fujitsu System Integration Laboratories Limited
Security Meister - High Master
Soya Aoyama

My Profile



SOYA AOYAMA

Security Researcher @ Fujitsu System Integration Laboratories Ltd
Organizer @ BSides Tokyo

1992 ~ 2015

software developer of Windows.

2015 ~

security researcher

- 2016 AVTOKYO
- 2017 BSides Las Vegas
- 2018 GrrCON / ToorCon / DerbyCon / AVTOKYO
- 2019 HackMiami / LeHack

2018 ~

BSides Tokyo Organizer

- 2018 first BSides in East Asia



What is a Local Hacking?

- Attacks that
 - after breaking into local PC
 - without regard administrator privileges



My research history



How to escalate privileges to administrator in latest Windows"

How to escalate privileges to administrator in latest Windows.

BSides Las Vegas 2017

July 25, 2017

Soya Aoyama



- Basic Concept
- Detail

It all started...

When I execute the CompMgmtLauncher

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-2JREPGP\saoyama]

File Options View Process Find DLL Users Help

Process	CPU	Private ...	Working ...	PID	Description	Company Name	Integrity
audiodg.exe		5,972 K	8,756 K	4000	Windows Audio Device Gr...	Microsoft Corporation	System
CompMgmtLauncher.exe		2,592 K	17,056 K	4136	Computer Management S...	Microsoft Corporation	High
csrss.exe		1,364 K	5,324 K	360	Client Server Runtime Pr...	Microsoft Corporation	System
csrss.exe	0.25	1,696 K	11,392 K	4424	Client Server Runtime Pr...	Microsoft Corporation	System

Name	Description	Company Na...	Path
ShellExtensionX64.dll			C:\Program Files\WinMerge\ShellExtensionX64.dll
[6AF0698E-D558-4F6E...			C:\ProgramData\Microsoft\Windows\Caches\[6AF0698E-D5...
[DDF571F2-BE98-426D...			C:\ProgramData\Microsoft\Windows\Caches\[DDF571F2-B...
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
[AFBF9F1A-8EE8-4C77...			C:\Users\saoyama\AppData\Local\Microsoft\Windows\Cac...
StaticCache.dat			C:\Windows\Fonts\StaticCache.dat
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls

CPU Usage: 3.43% Commit Charge: 25.12% Processes: 51 Physical Usage: 38.71%

CompMgmtLauncher.exe

- does not display the UAC screen
- executes with administrator privileges
- loads 3rd Party dll (in Program Files Folder)

What processes can access programmer's folder?

- Explorer.exe?

So...

I checked the Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-2JREPGP\saoyama]

File Options View Process Find DLL Users Help

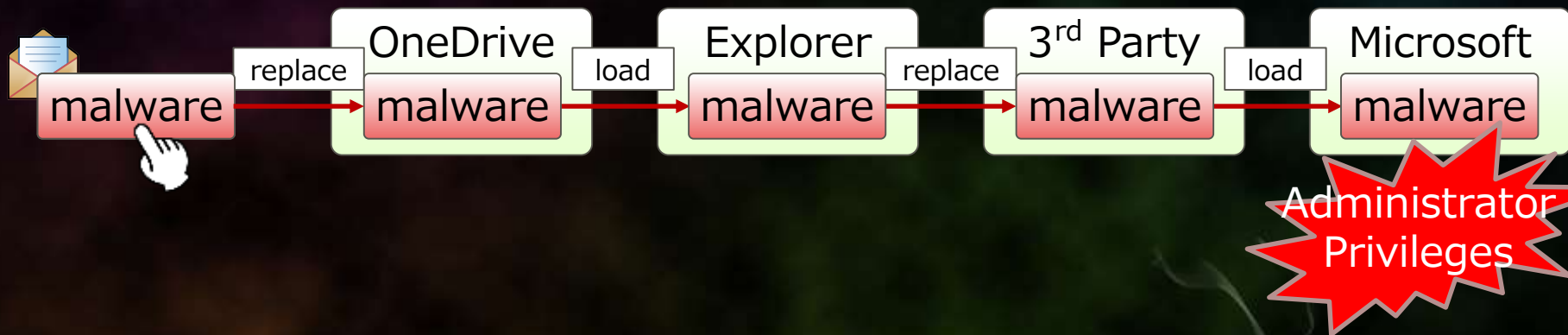
Process	CPU	Private ...	Working ...	PID	Description	Company Name	Integrity
explorer.exe	0.07	36,064 K	108,288 K	4720	Windows Explorer	Microsoft Corporation	Medium
Interrupts	0.29	0 K	0 K	n/a	Hardware Interrupts and ...		
lsass.exe		4,920 K	14,376 K	532	Local Security Authority ...	Microsoft Corporation	System
Memory Compression		76 K	2,480 K	1712			System

Name	Description	Company Na...	Path
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
ClientTelemetry.dll			C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
FileSyncShell64.dll	Microsoft OneDrive...	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
LoggingPlatform...	Logging Platform	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
msvcp120.dll	Microsoft® C Runti...	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
msvcr120.dll	Microsoft® C Runti...	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
{3DA71D5A-20C...			C:\Users\saoyama\AppData\Local\Microsoft\Windows\Caches\{...
{AFBF9F1A-8EE...			C:\Users\saoyama\AppData\Local\Microsoft\Windows\Caches\{...

CPU Usage: 5.96% Commit Charge: 24.35% Processes: 49 Physical Usage: 37.91%

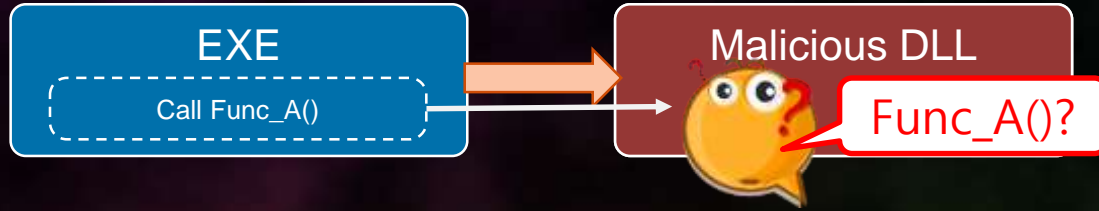
Which means...

I found a way to get administrator privileges

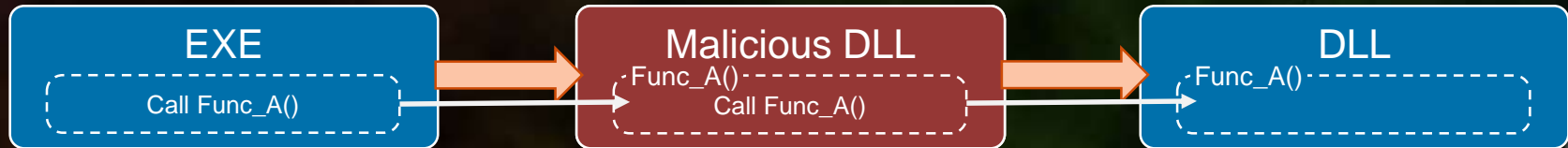


Basic Concept

Replace the correct dll with malicious one



Pass through the function to the correct dll



What functions the dll has

I used the dumpbin command

```
開発者コマンドプロンプト for VS 2017
File Type: DLL
Section contains the following exports for File Type: DLL
00000000 characteristics
FFFFFFFF time date stamp
0.00 version
1 ordinal base
5 number of functions
5 number of names

ordinal hint RVA      name
1 0 000065E0 DllCanUnloadNow
2 1 00006620 DllGetClassObject
3 2 00006780 DllRegisterServer
4 3 00006860 DllUnregisterServer
5 4 000037A0 Test_IsMemberOf

Summary
A000 .data
8000 .pdata
3A000 .rdata
2000 .reloc
A2000 .rsrc
77000 .text

C:\Program Files (x86)\Microsoft Visual Studio
```

```
開発者コマンドプロンプト for VS 2017
File Type: DLL
Section contains the following exports for ShellExtensionX64.DLL
00000000 characteristics
FFFFFFFF time date stamp
0.00 version
1 ordinal base
4 number of functions
4 number of names

ordinal hint RVA      name
1 0 00006778 DllCanUnloadNow
2 1 00006784 DllGetClassObject
3 2 00006854 DllRegisterServer
4 3 00006868 DllUnregisterServer

Summary
3000 .data
2000 .pdata
D000 .rdata
1000 .reloc
D000 .rsrc
15000 .text

C:\Program Files (x86)\Microsoft Visual Studio\2017\Enterprise>
```

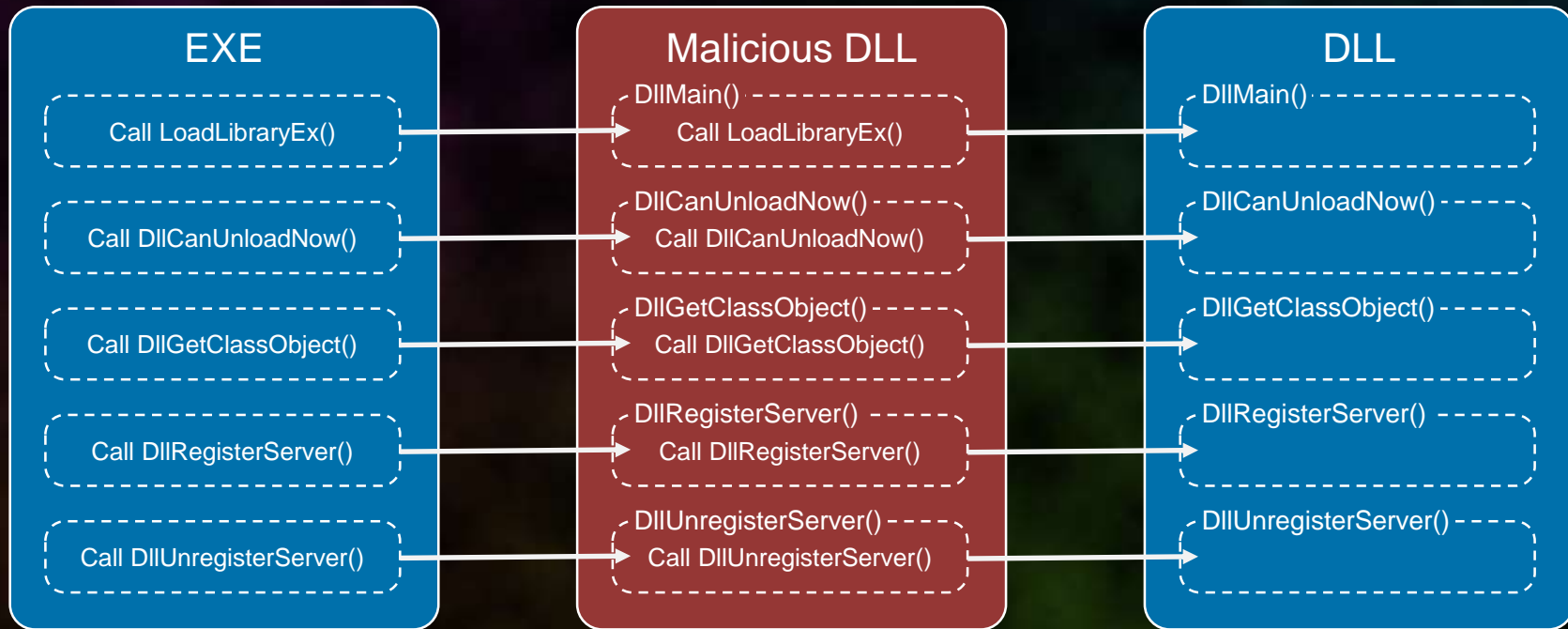
The four functions API

Describe on Microsoft web site.

- HRESULT DllCanUnloadNow(void);
- HRESULT DllGetClassObject(REFCLSID rclsid, REFIID riid, LPVOID *ppv);
- HRESULT DllRegisterServer(void);
- HRESULT DllUnregisterServer (void);

So...

Only need to implement four functions



To realize concept

the implementation necessary

1. Load the correct DLL and get its handle


```
hModule = LoadLibraryEx(lpLibFileName, hFile, dwFlags);
```

2. Get address of each function using handle

```
Address = GetProcAddress(hModule, lpProcName);
```

3. When called from EXE, call the corresponding function with the correct arguments

```
return Address(arg1, arg2, ...);
```



Source Code

It does not contain malicious code

```
#include <Shobjidl.h>

typedef HRESULT(__stdcall *CUN)(void);
typedef HRESULT(__stdcall *GCO)(REFCLSID rclsid, REFIID riid, LPVOID *ppv);
typedef HRESULT(__stdcall *RS)(void);
typedef HRESULT(__stdcall *US)(void);
CUN CanUnloadNow;
GCO GetClassObject;
RS RegisterServer;
US UnregisterServer;

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_for_call, LPVOID lpReserved)
{
    if (DLL_PROCESS_ATTACH == ul_reason_for_call) {
        WCHAR dll[MAX_PATH + 1] = { 0 };
        GetModuleFileName(hModule, dll, MAX_PATH);
        wscat(dll, L"\\");
        HINSTANCE hDllInstance = ::LoadLibraryEx(dll, NULL, LOAD_WITH_ALTERED_SEARCH_PATH);
        CanUnloadNow = (CUN)GetProcAddress(hDllInstance, "DllCanUnloadNow");
        GetClassObject = (GCO)GetProcAddress(hDllInstance, "DllGetClassObject");
        RegisterServer = (RS)GetProcAddress(hDllInstance, "DllRegisterServer");
        UnregisterServer = (US)GetProcAddress(hDllInstance, "DllUnregisterServer");
    }
    return TRUE;
}

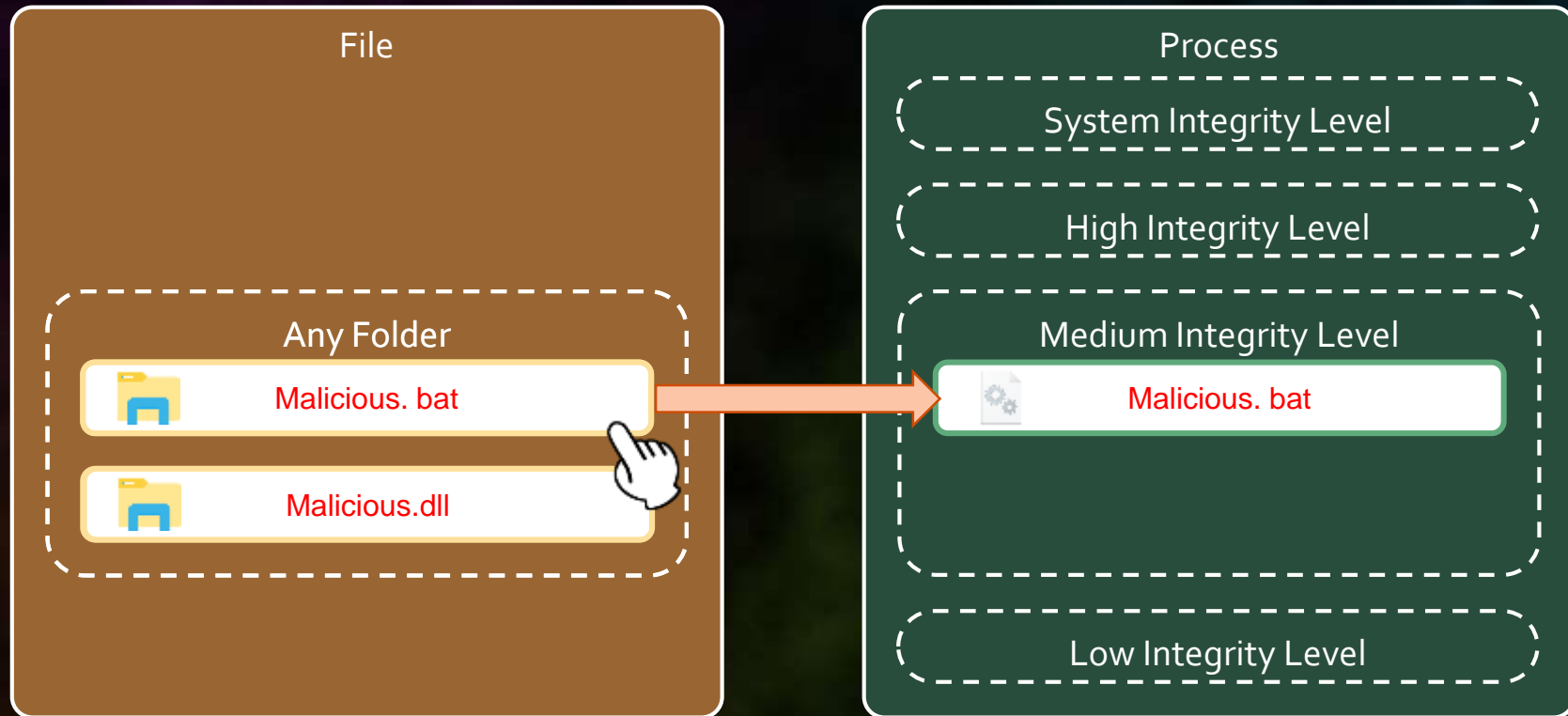
STDAPI DllCanUnloadNow(void) { return CanUnloadNow(); }
STDAPI DllGetClassObject(REFCLSID rclsid, REFIID riid, LPVOID *ppv) { return GetClassObject(rclsid, riid, ppv); }
STDAPI DllRegisterServer(void) { return RegisterServer(); }
STDAPI DllUnregisterServer(void) { return UnregisterServer(); }
```

Demonstration video 1



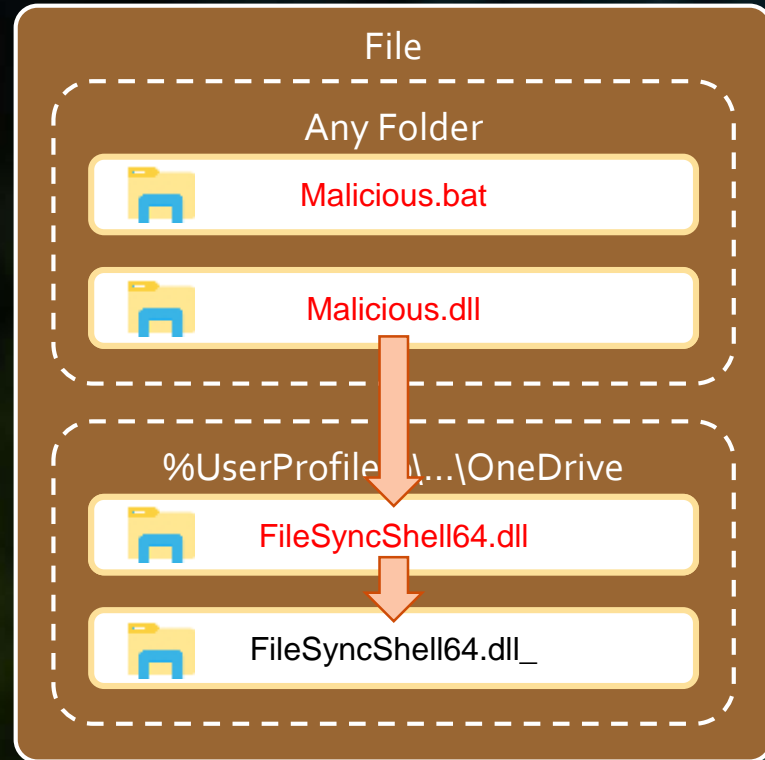
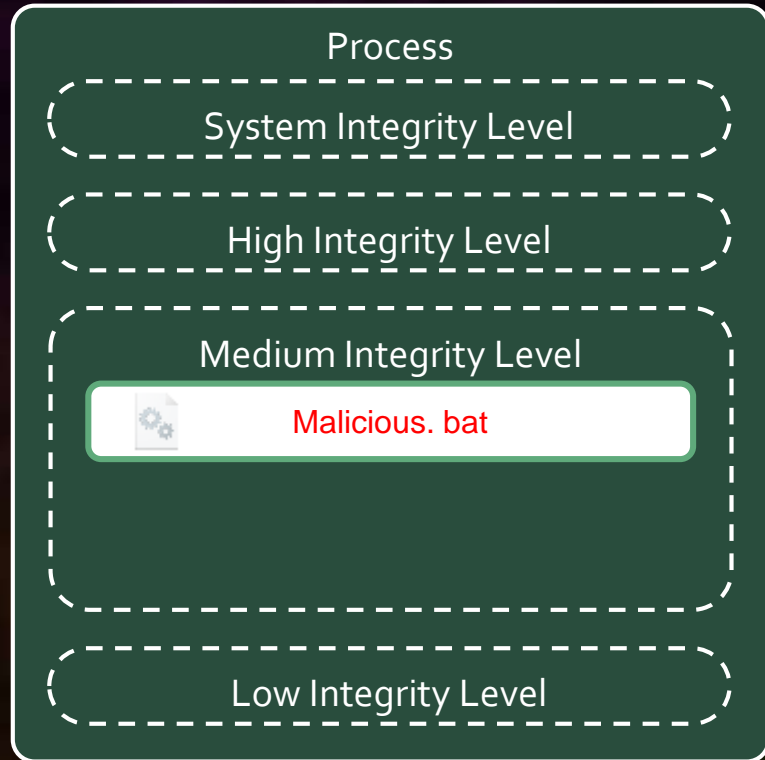
Mechanism

User executes malicious program



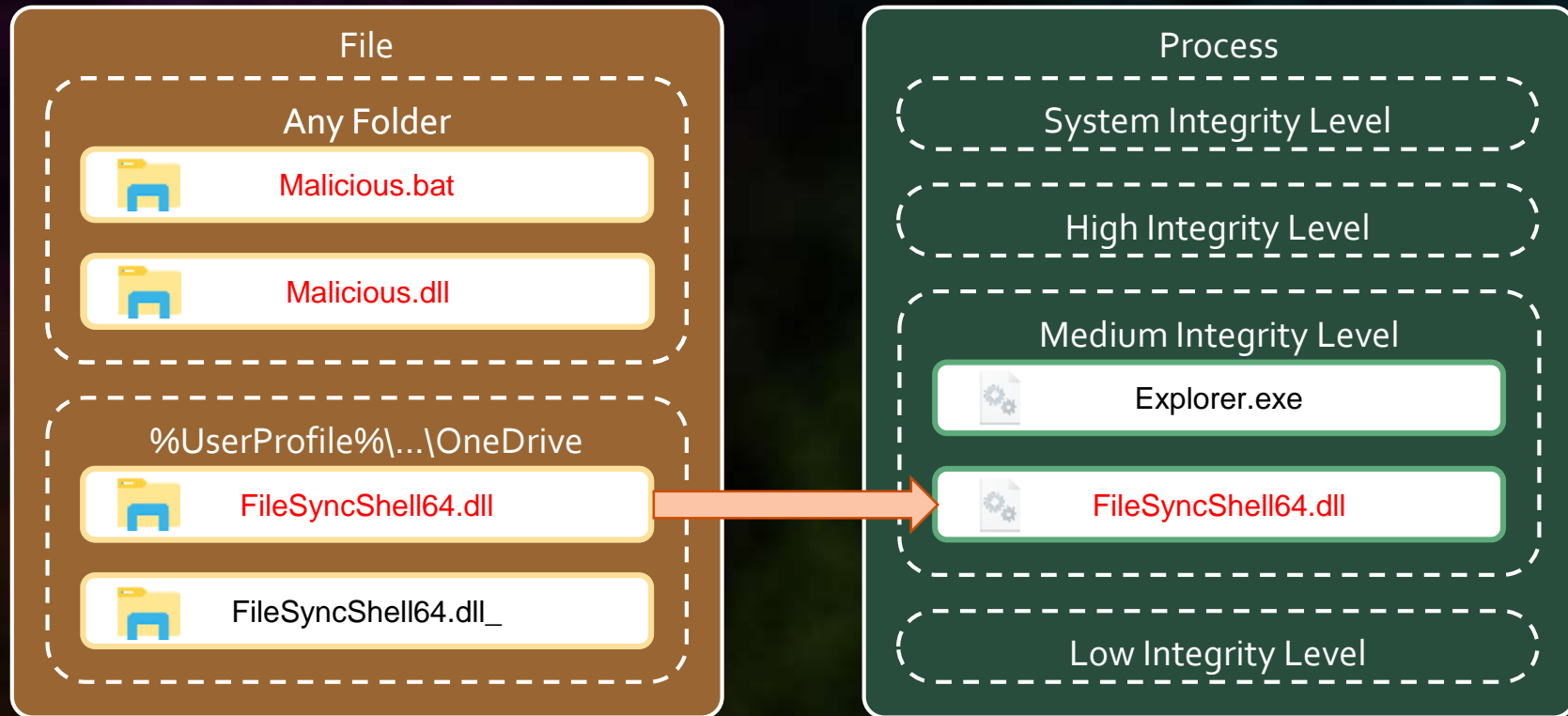
Mechanism

Malicious program replaces correct dll with itself



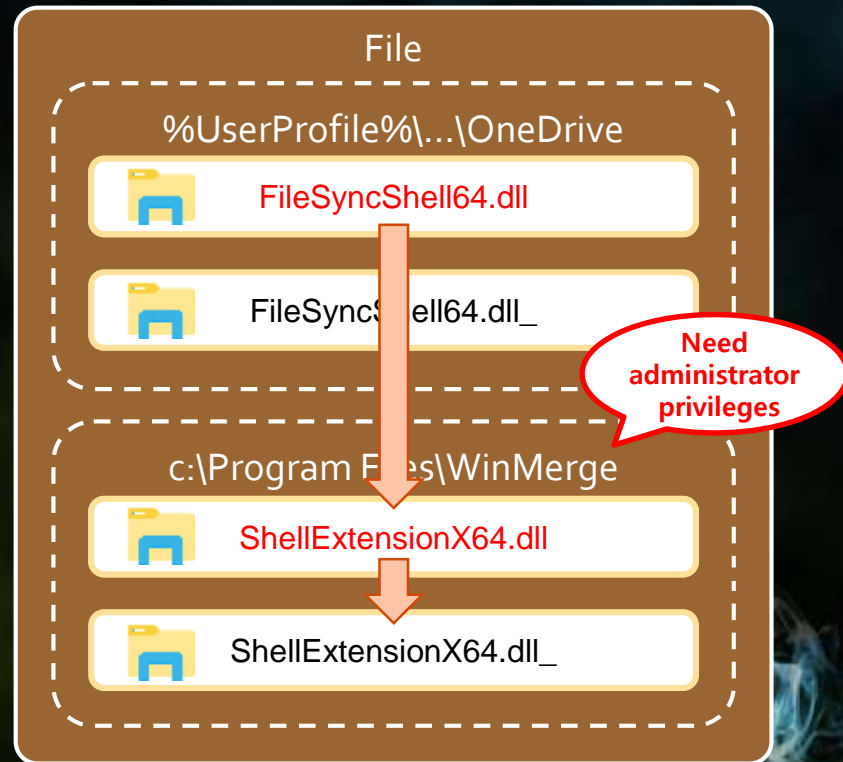
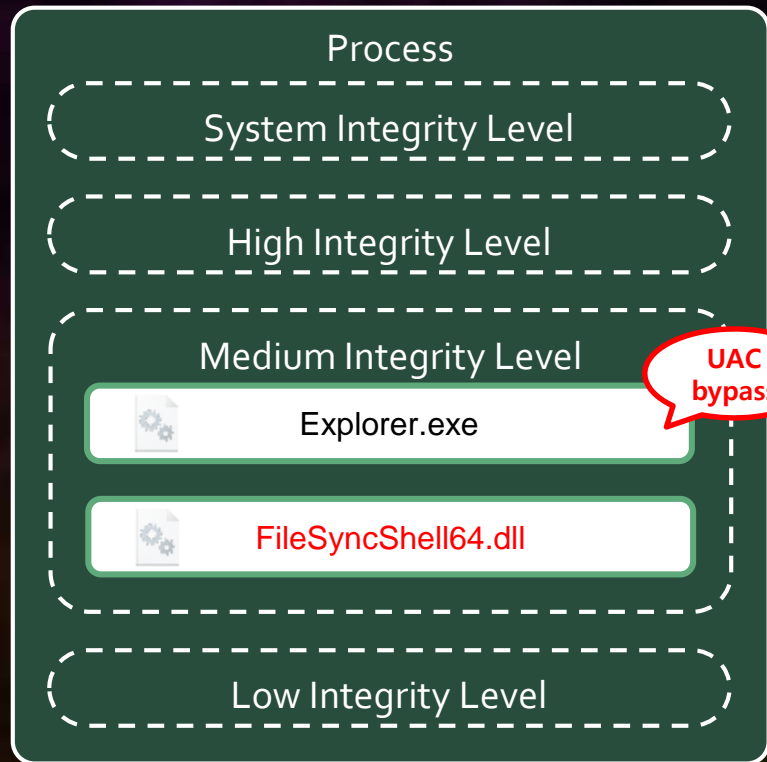
Mechanism

Explorer loads malicious dll



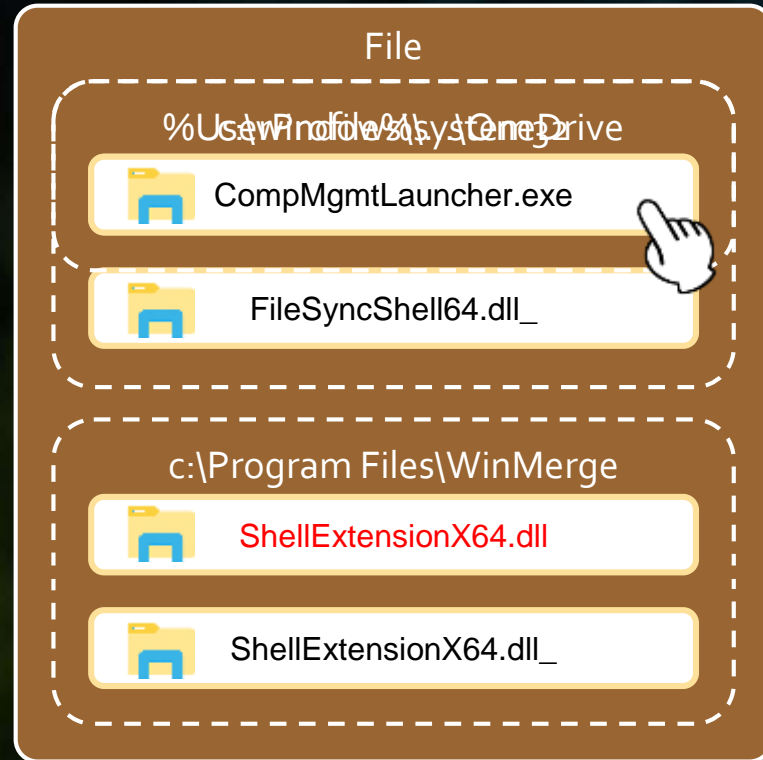
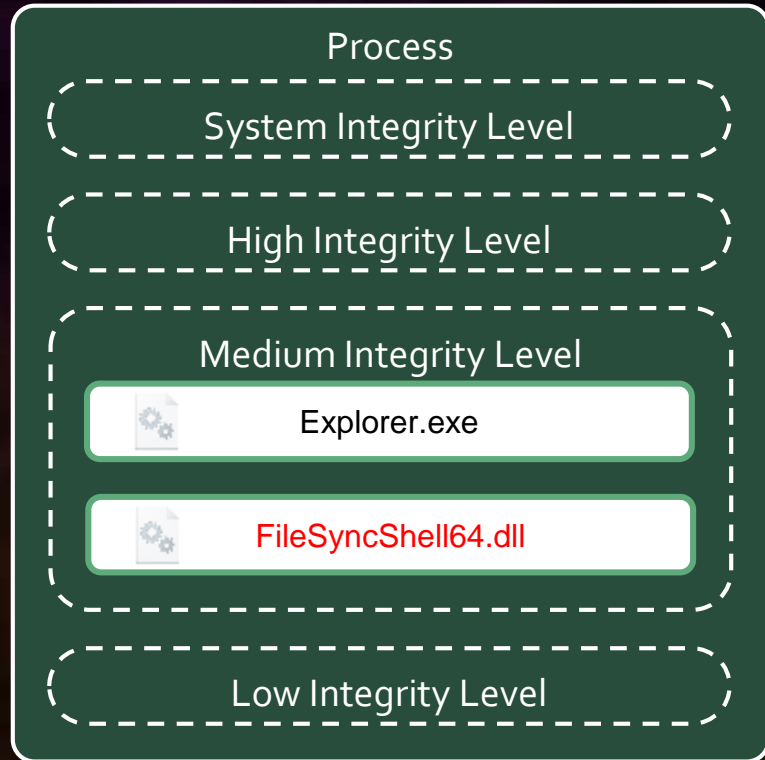
Mechanism

Malicious program replaces correct dll with itself



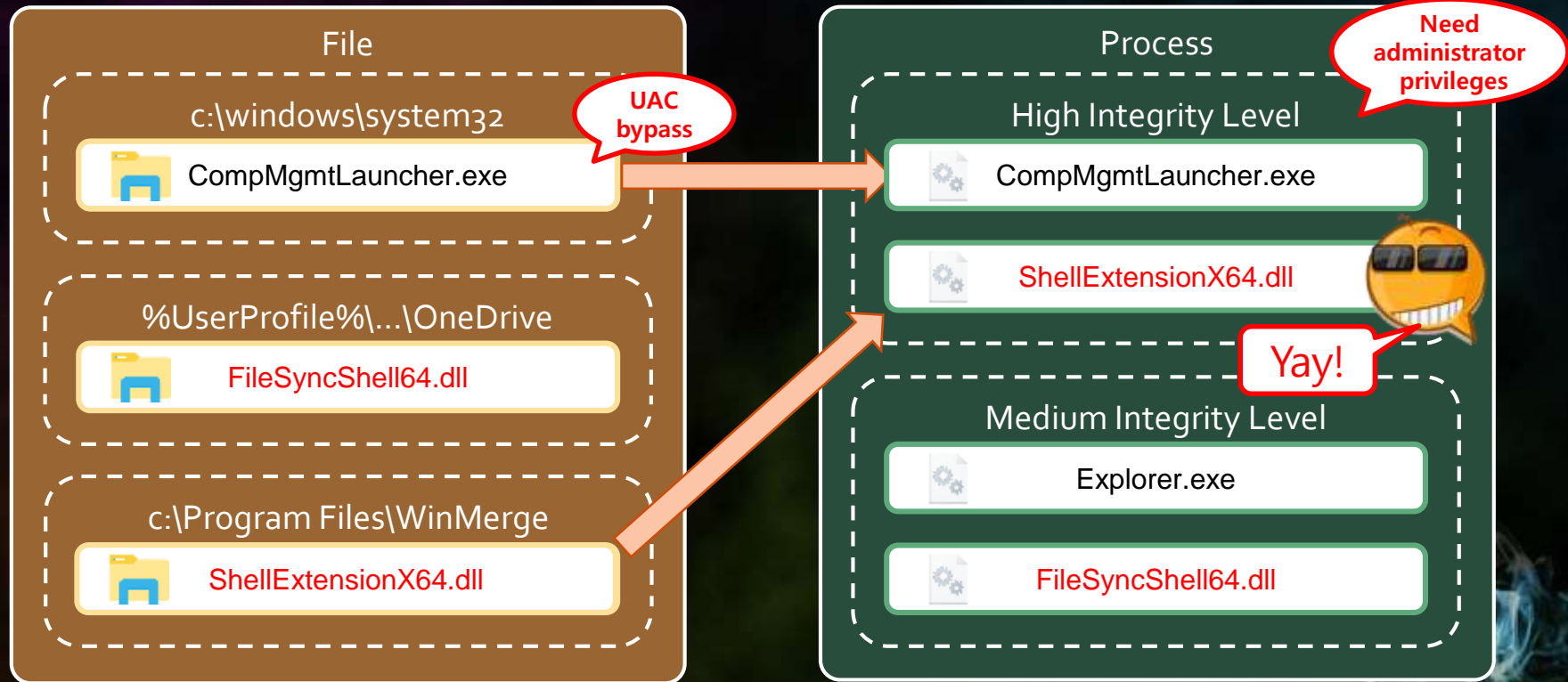
Mechanism

Malicious program executes CompMgmtLauncher



Mechanism

Malicious program gets administrative privileges



Bug Bounty Program

Microsoft Bug Bounty Program

Microsoft strongly believes close partnerships with researchers make customers more secure. Security researchers play an integral role in the ecosystem by discovering vulnerabilities missed in the software development process. Each year we partner together to better protect billions of customers worldwide.

The Microsoft Bug Bounty Program is designed to supplement and encourage research in certain technologies to better protect our customers and the broader ecosystem. Through targeted and ongoing bounty programs, we reward researchers for submitting their findings to one of our eligible bounty programs and for partnering with us through [Coordinated Vulnerability Disclosure](#). If you are a security researcher that has found a vulnerability in a Microsoft product, service, or device we want to hear from you. If it is within scope of a bounty program you can receive bounty award according to the program descriptions. Even if it is not covered under an existing bounty program, we will publicly acknowledge your contributions when we fix the vulnerability. Both categories of submission are counted in our annual [Top 100 Researcher](#) leaderboard.

[Click here to submit a security vulnerability](#)

<https://www.microsoft.com/en-us/msrc/bounty?rtc=1>

**I submitted a vulnerability report
MSRC said...**

MSRC said...

can **not** pay the reward



Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). Upon investigation, we have determined that **this does not meet the bar for security servicing** as binary planting in the application directory would already indicate the user is compromised.

For an in-depth discussion of what constitutes a product vulnerability please see the following:

"Definition of a Security Vulnerability"

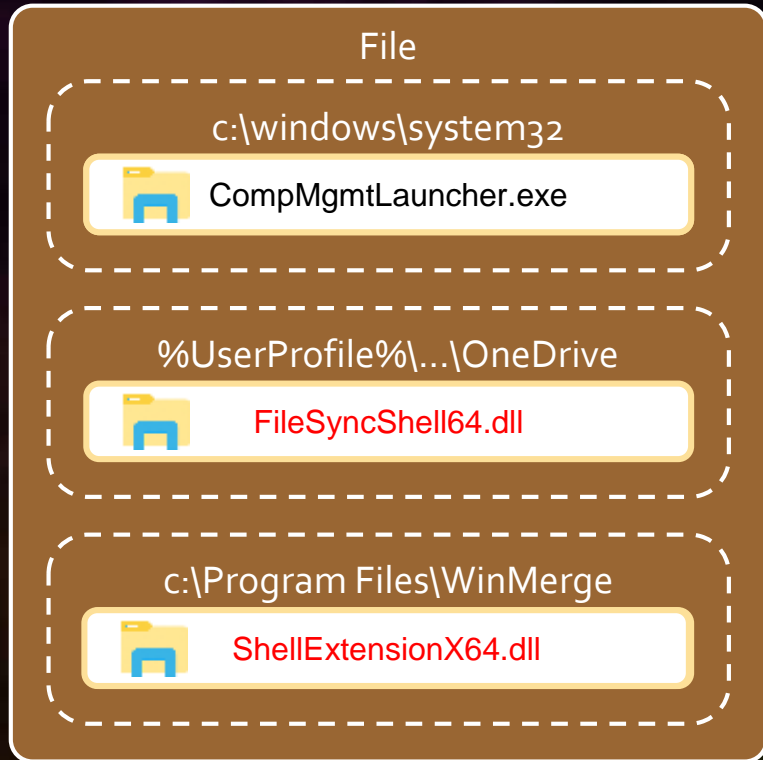
<<https://technet.microsoft.com/library/cc751383.aspx>>

Again, we appreciate your report.

Regards,

However...

This issue has been fixed



Microsoft quietly fixed!!



How important is administrator privilege?

- Little change in what an attacker can do
- A lot of data locally

**Attacks that do not require
administrator privileges**

 **The Local Hacking**

An Inconvenient Truth:

Evading the Ransomware Protection in Windows10

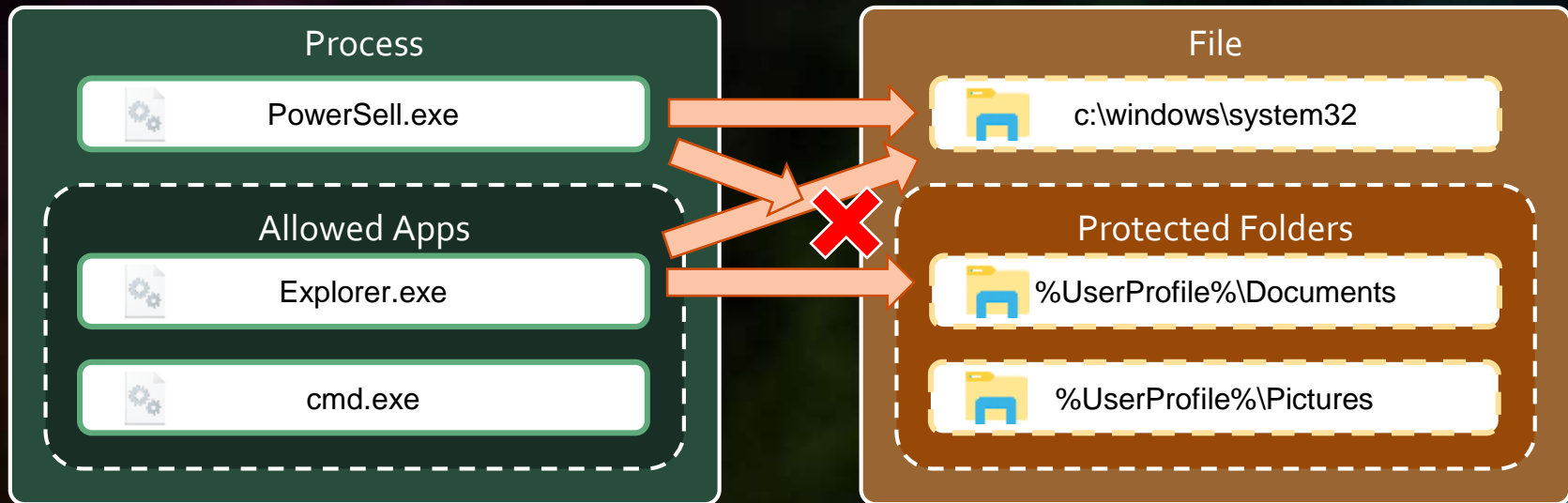
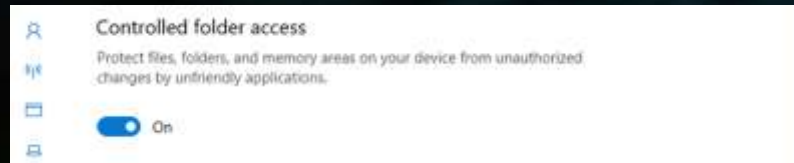
An Inconvenient Truth:

*Evading the Ransomware Protection
in Windows 10*

- Basic Concept
- Detail

I noticed ...

There is a defect in Ransomware Protection



It all started ...

Why does Explorer load OneDrive dll?

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-2JREPGP\saoyama]

File Options View Process Find DLL Users Help

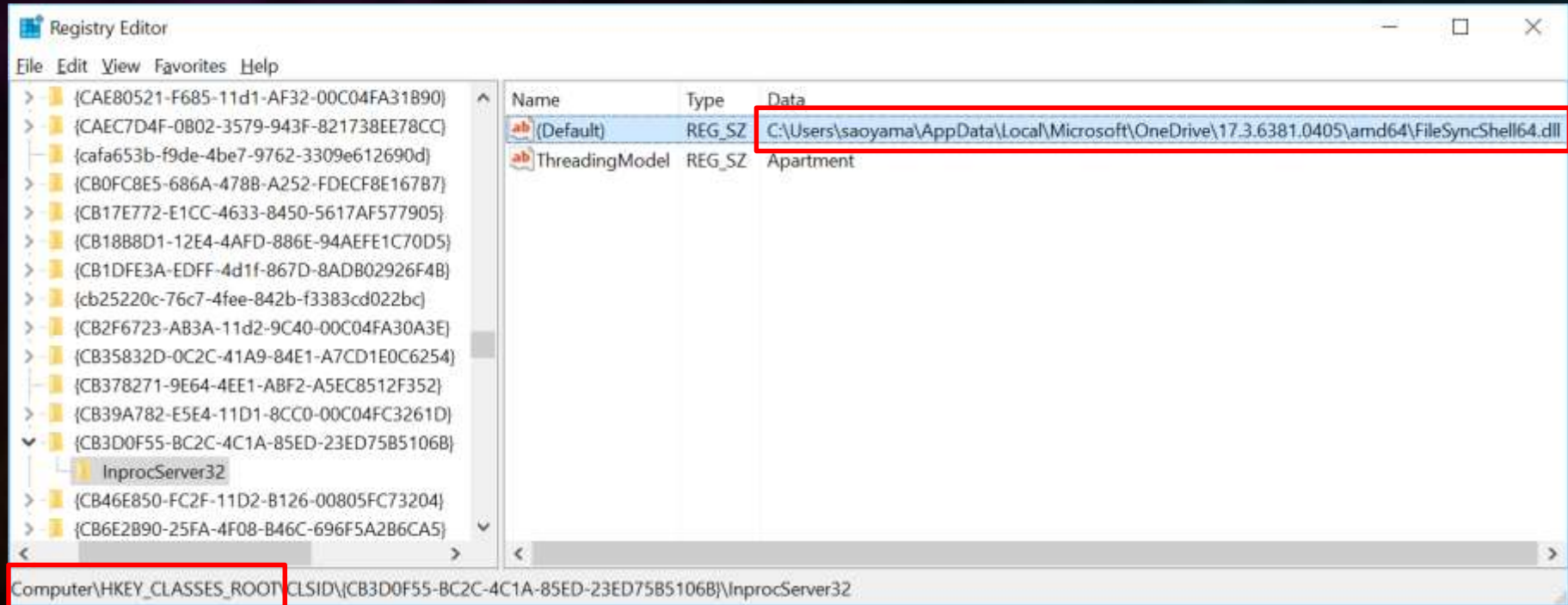
Process	CPU	Private ...	Working ...	PID	Description	Company Name	Integrity
explorer.exe	0.07	36,064 K	108,288 K	4720	Windows Explorer	Microsoft Corporation	Medium
Interrupts	0.29	0 K	0 K	n/a	Hardware Interrupts and ...		
lsass.exe		4,920 K	14,376 K	532	Local Security Authority ...	Microsoft Corporation	System
Memory Compression		76 K	2,480 K	1712			System

Name	Description	Company Na...	Path
cversions.2.db			C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db
ClientTelemetry.dll			C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
FileSyncShell64.dll	Microsoft OneDrive...	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
LoggingPlatform...	Logging Platform	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
msvcp120.dll	Microsoft® C Runti...	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
msvcr120.dll	Microsoft® C Runti...	Microsoft Co...	C:\Users\saoyama\AppData\Local\Microsoft\OneDrive\17.3.638...
{3DA71D5A-20C...			C:\Users\saoyama\AppData\Local\Microsoft\Windows\Caches\{...
{AFBF9F1A-8EE...			C:\Users\saoyama\AppData\Local\Microsoft\Windows\Caches\{...

CPU Usage: 5.96% Commit Charge: 24.35% Processes: 49 Physical Usage: 37.91%


I searched in the registry

It was found in HKEY_CLASSES_ROOT



What HKEY_CLASSES_ROOT?

HKCR is that merges HKLM with HKCU

 Microsoft

Windows Dev Center

Windows PCs


Docs

Downloads

Samples

Support


Dashboard

Search 

Docs / Windows / Windows System Information / Registry / About the Registry / Predefined Keys / Merged View of HKEY_CLASSES_ROOT

Share Theme Sign in

Merged View of HKEY_CLASSES_ROOT

05/31/2018 • 2 minutes to read • Contributors 

The [RegOpenUserClassesRoot](#) function provides a merged view for processes, such as services, that are dealing with clients other than the interactive user. In this case, the HKEY_CLASSES_ROOT key provides a view of the registry that merges the information from HKEY_LOCAL_MACHINE\Software\Classes with the information from HKEY_CURRENT_USER\Software\Classes.

The system uses the following rules to merge information from the two sources:

- The merged view includes all subkeys of the HKEY_CURRENT_USER\Software\Classes key.
- The merged view includes all immediate subkeys of the HKEY_LOCAL_MACHINE\Software\Classes key that do not duplicate the subkeys of HKEY_CURRENT_USER\Software\Classes.
- At the end of this topic is a list of subkeys that are found in both HKEY_LOCAL_MACHINE\Software\Classes and HKEY_CURRENT_USER\Software\Classes. The immediate subkeys of these keys from the HKEY_LOCAL_MACHINE tree are included in the merged view only if they are not duplicates of immediate subkeys from the HKEY_CURRENT_USER tree. The merged view does not include the HKEY_LOCAL_MACHINE contents of duplicate subkeys.

<https://docs.microsoft.com/en-us/windows/desktop/sysinfo/merged-view-of-hkey-classes-root>

Which dll meets the requirements?

I found it

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-2JREPGP\saoiyama]

File Options View Process Find DLL Users Help

Process	CPU	Private...	Working...	PID	Description	Company Name	Integrity
explorer.exe	0.06	31,828 K	86,652 K	3608	Windows Explorer	Microsoft Corporation	Medium

Name	Description	Company Name	Path
shell32.dll	Windows Shell Common DLL	Microsoft Corporation	C:\Windows\System32\shell32.dll
shlwapi.dll	Shell		
slc.dll	Soft		

CPU Usage: 5.16%

Registry Editor

File Edit View Favorites Help

Name	Type	Data
(Default)	REG_E...	%SystemRoot%\system32\shell32.dll

Registry Editor

File Edit View Favorites Help

Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID

What functions the dll has

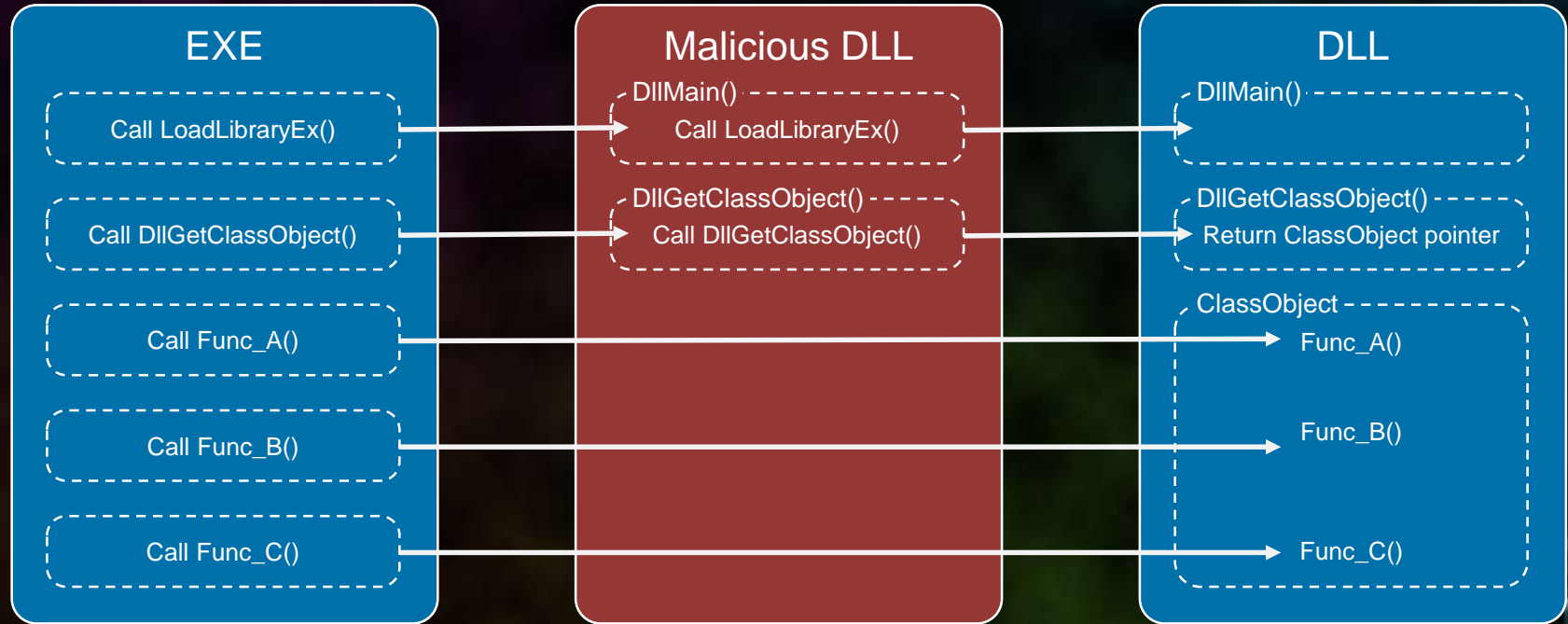
I used the dumpbin command

```
開発者コマンドプロンプト for VS 2017
File Type: DLL
Section contains the following exports for SHELL32.dll
00000000 characteristics
6A056922 time date stamp
0.00 version
2 ordinal base
2000 number of functions
482 number of names

ordinal hint RVA      name
255 0 001F18E0 AppCompat_RunDLLW
263 1 0006C610 AssocCreateForClasses
267 2 001F8780 AssocGetDetailsOfPropKey
701 3 001FF250 CDefFolderMenu_Create2
83 4 00200170 CIDLData_CreateFromIDArray
937 5 00197B60 CStorageItem_GetValidatedStorageItemObject
268 6 00205630 CheckEscapesW
269 7 000BB6B0 CommandLineToArgvW
272 8 00207E70 Control_RunDLL
273 9 00207E70 Control_RunDLLA
274 A 00207EF0 Control_RunDLLAsUserW
275 B 00207F30 Control_RunDLLW
935 C 00197BA0 CreateStorageItemFromPath_FullTrustCaller
936 D 00197BC0 CreateStorageItemFromPath_FullTrustCaller_ForPackage
920 E 00197BE0 CreateStorageItemFromPath_PartialTrustCaller
```

However...

Only need to implement four export functions

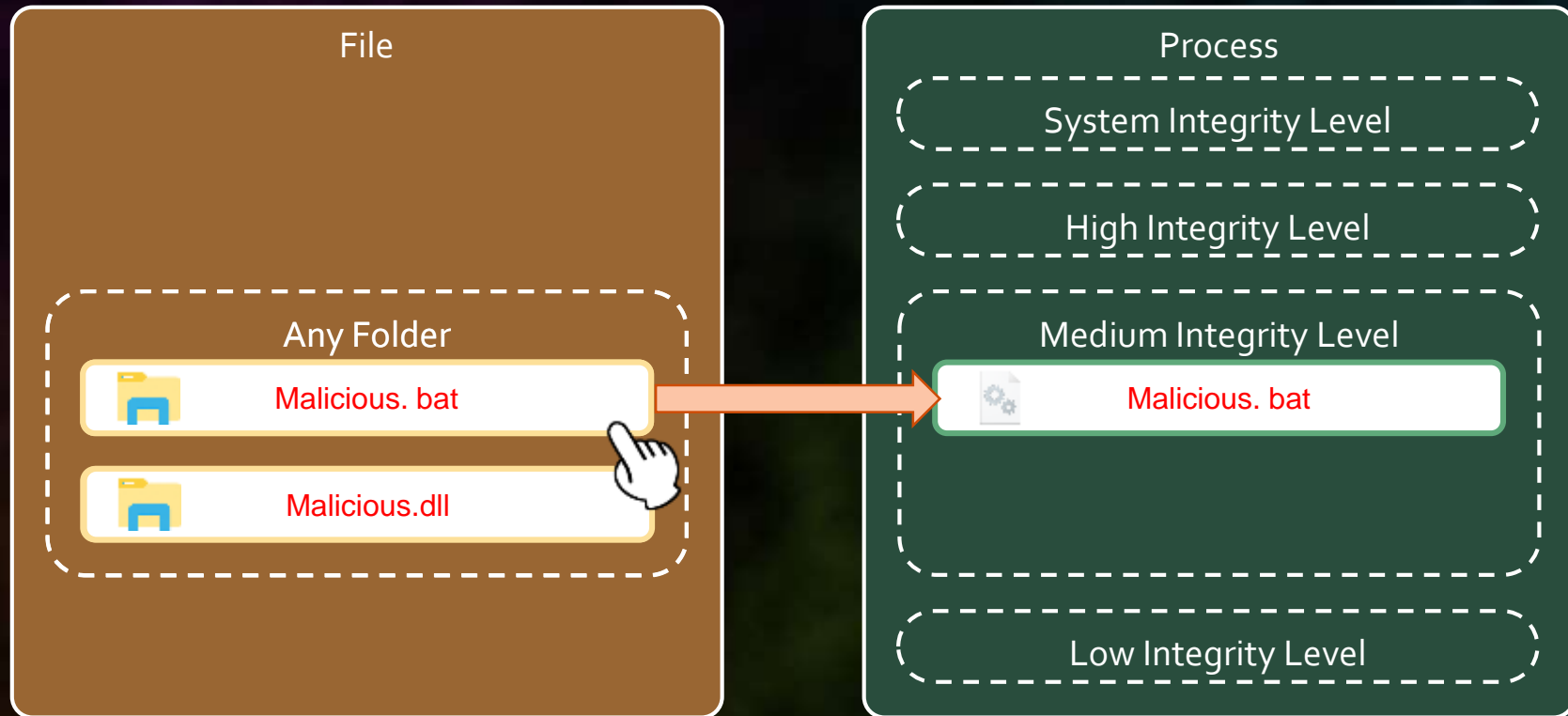


Demonstration video 2



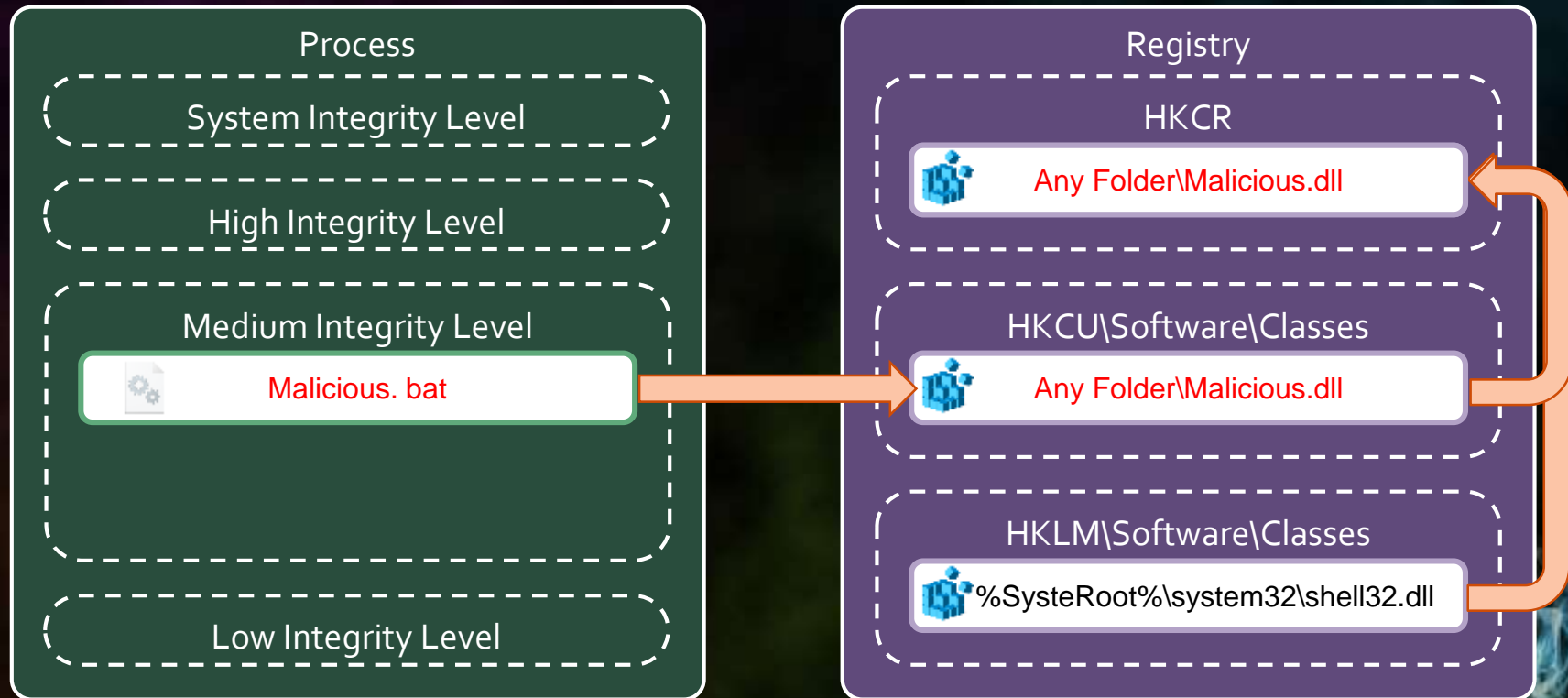
Mechanism

User executes malicious program



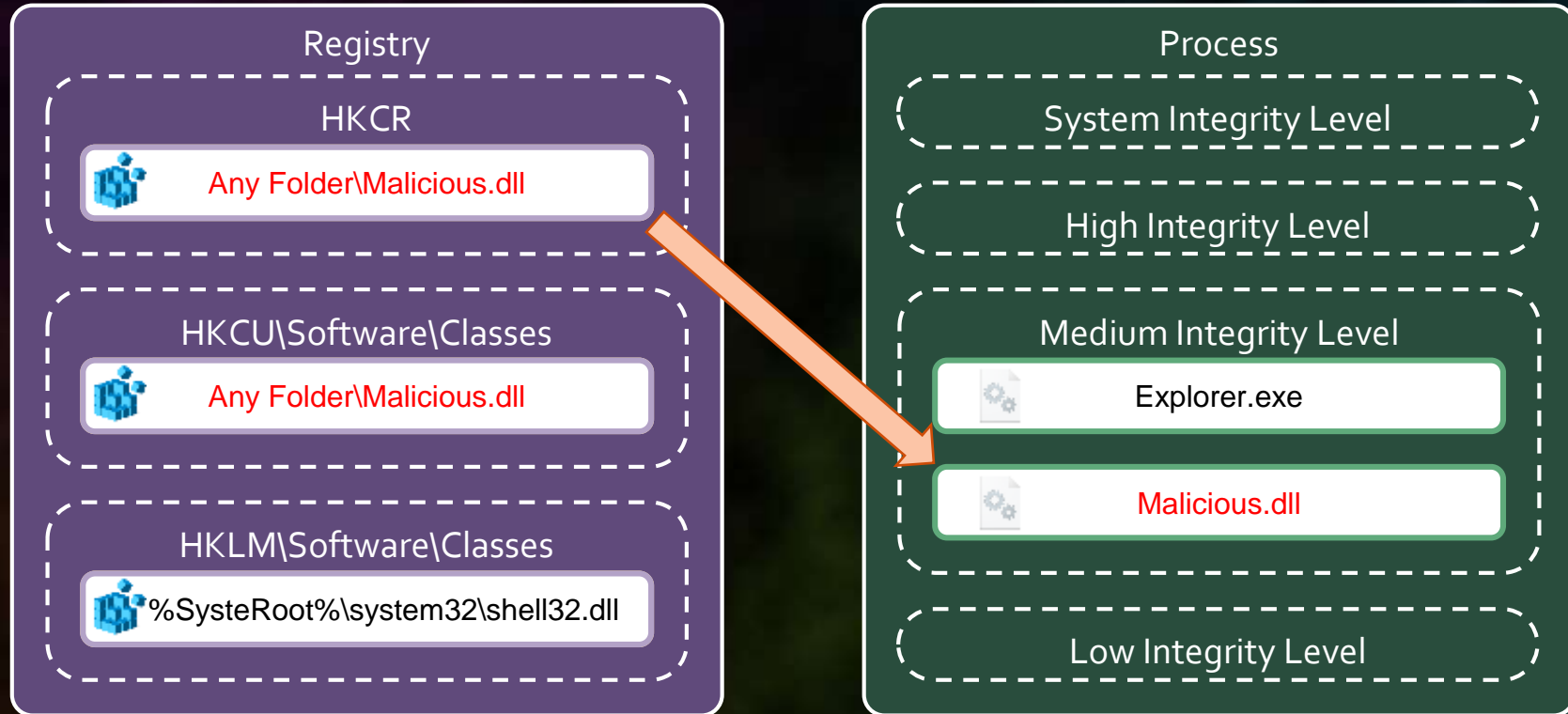
Mechanism

Malicious program writes malicious path to HKCU



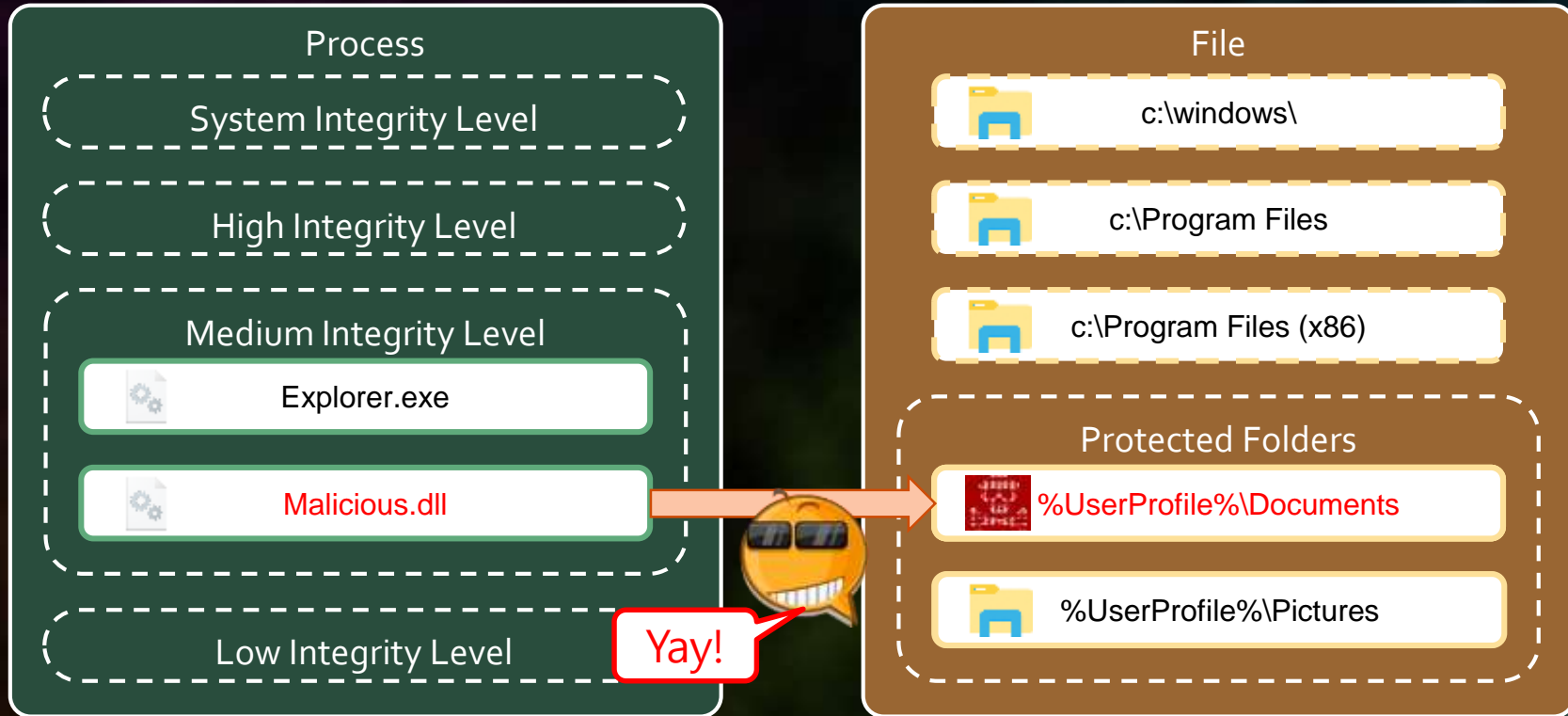
Mechanism

Explorer loads malicious dll



Mechanism

Malicious dll encrypts files in Protected Folders



It's revenge
I submitted a vulnerability report
MSRC said...



MSRC said...

can **not** pay the reward



Hello,

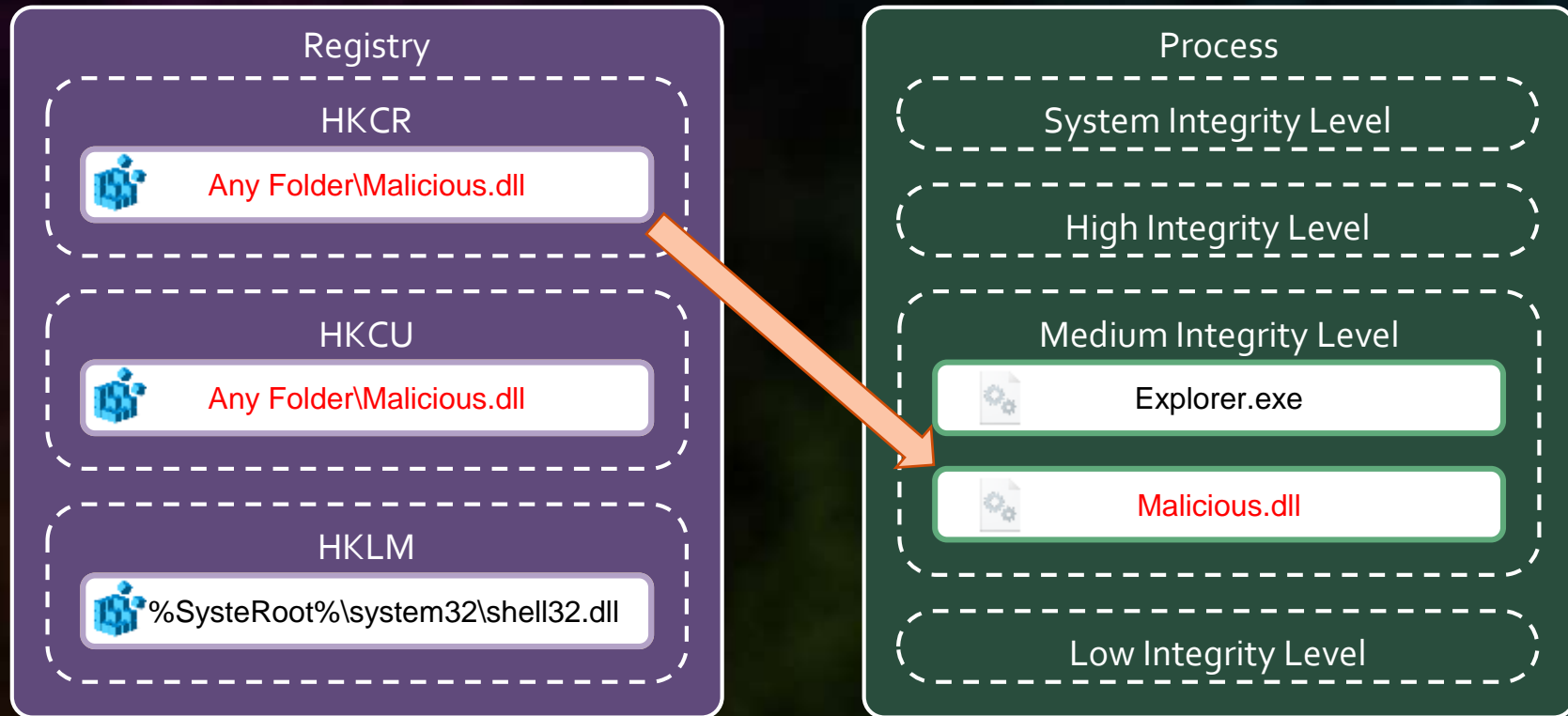
Thank you for contacting the Microsoft Security Response Center (MSRC). If I am interpreting correctly, this report is predicated on the attacker having login access to the target's account already. Forged by planting a dll through registry modifications. Since you are only able to write to HKCU, you will not be able to effect other users, just the target you have already compromised through other means. There also does not appear to be an escalation of privileges and you already had the same access level as the target. It would appear the attacker would not gain anything from this attack and could already do anything that the planting could trigger. As your report as written **this does not meet the bar for security servicing.**

As such, this thread is being closed and no longer monitored.

If you believe this to be a misunderstanding of the report, submit a new email to secure@microsoft.com without a CRM number in the subject line. Please include:

By the way

Microsoft has not fixed this issue yet



Microsoft says...

- Local Hacking is not a vulnerability

Attackers can do whatever they want

➡ The Further Local Hacking



You Ain't Seen Nothin' Yet!



**Do you use the password
long enough and complexity?**



Don't tell me you use Post-it !!

A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note

Kif Leswing Jan. 16, 2018, 3:07 PM



AP/Composite/Rob Price

<https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1>

Don't tell me you reuse password !!

Github accounts Hacked in 'Password reuse attack'

June 17, 2016 Swati Khandelwal



<https://thehackernews.com/2016/06/github-password-hack.html>

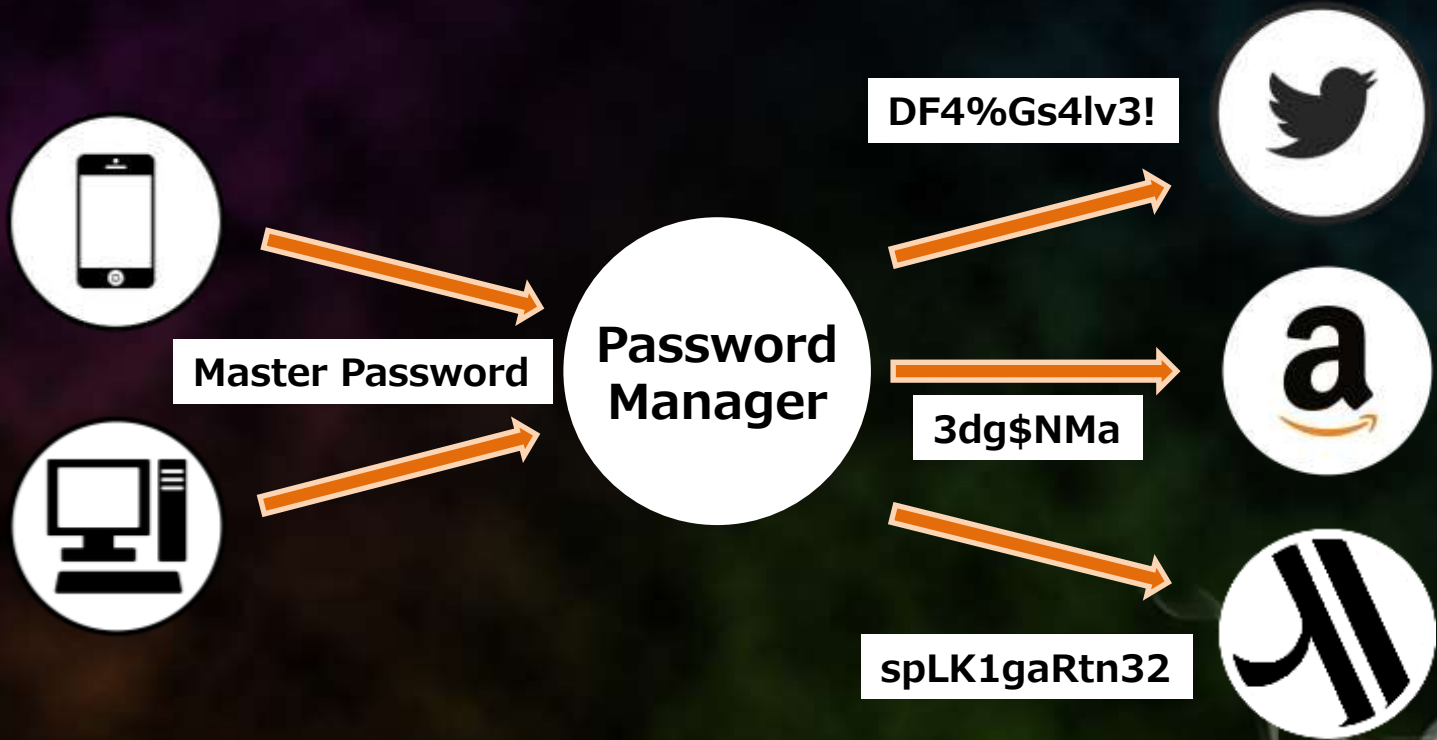
Our memory is not so good



**You use a password Manager,
right?**



What is a password manager?



There are various products

PC

REVIEWS ▾ BEST PICKS ▾ HOW-TO ▾ NEWS ▾ SMART HOME BUSINESS ▾ SHOP ▾

What are you looking for? 

 Computex2019  Huawei  Windows10MayUpdate  Verizon5GTested  PrimeDay

Subscribe:  

The Best Password Managers for 2019

Still using your kid's birthday as your universal password? You're heading toward trouble. With a password manager, you can have a unique and strong password for every secure website. We've evaluated two dozen of the best password managers to help you choose.

 By Neil J. Rubenking May 1, 2019 3:23PM EST

       15 SHARES

PCMag reviews products independently, but we may earn affiliate commissions from buying links on this page. [Terms of use.](#)

Product	Zoho Vault	Keeper Password Manager & Digital Vault	Dashlane	Sticky Password Premium	LastPass Premium	Password Boss	LogMeOnce Password Management Suite Ultimate	RoboForm 8 Everywhere	AgileBits 1Password	True Key by Intel Security
										

<https://www.pcmag.com/roundup/300318/the-best-password-managers>

Oh my...

There are exe and dll in Users folder

Process Explorer - Sysinternals: www.sysinternals.com [MARS0013-01\$saoyama]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Integrity
ApplicationFrameHost.exe		16,836 K	17,636 K	10948	Application Frame Host	Microsoft Corp...	Medium

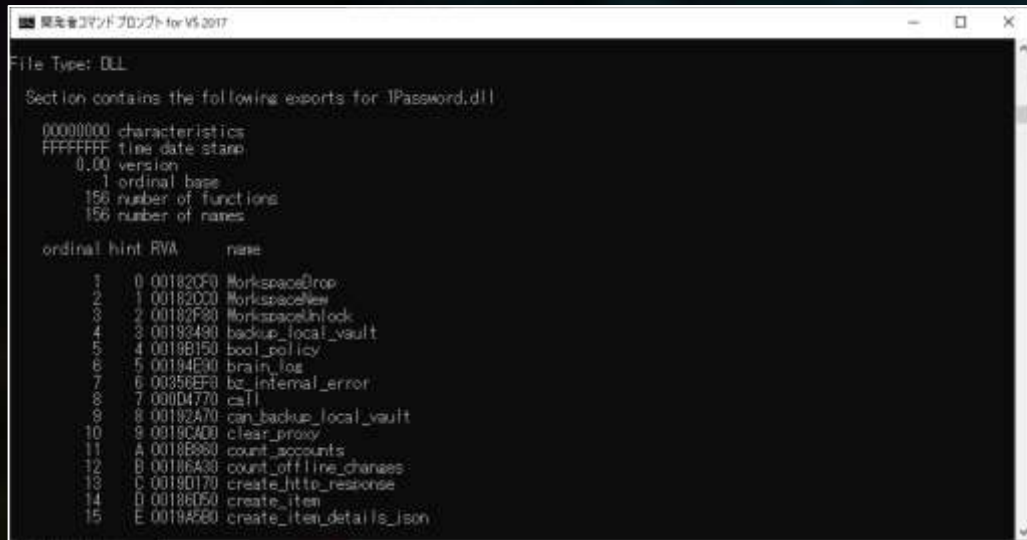
Name	Description	Company Name	Path
.dll			C:\Users\saoyama\AppData\Local\
.exe			C:\Users\saoyama\AppData\Local\
{AFBF9F1A-8...			C:\Users\saoyama\AppData\Local\Microsoft\Windows\Caches\{AFB...
Accessibility.n...	.NET Framework	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\Accessibility\7...
mscorlib.ni.dll	Microsoft Common Language Ru...	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\898...
PresentationF...	PresentationFramework.dll	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentation5ae...
PresentationF...	PresentationFramework.Aero2.dll	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentationaec...
PresentationC...	PresentationCore.dll	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCo...
System.Config...	System.Configuration.dll	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configu...
System.Core....	.NET Framework	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\7...
Svstem.Drawi...	.NET Framework	Microsoft Corp...	C:\Windows\assembly\NativeImages_v4.0.30319_32\Svstem.Drawin...

CPU Usage: 6.66% Commit Charge: 44.77% Processes: 197 Physical Usage: 61.61%

xxxx.dll

Does not have following export functions

- DllCanUnloadNow()
- DllGetClassObject()
- DllRegisterServer()
- DllUnregisterServer()



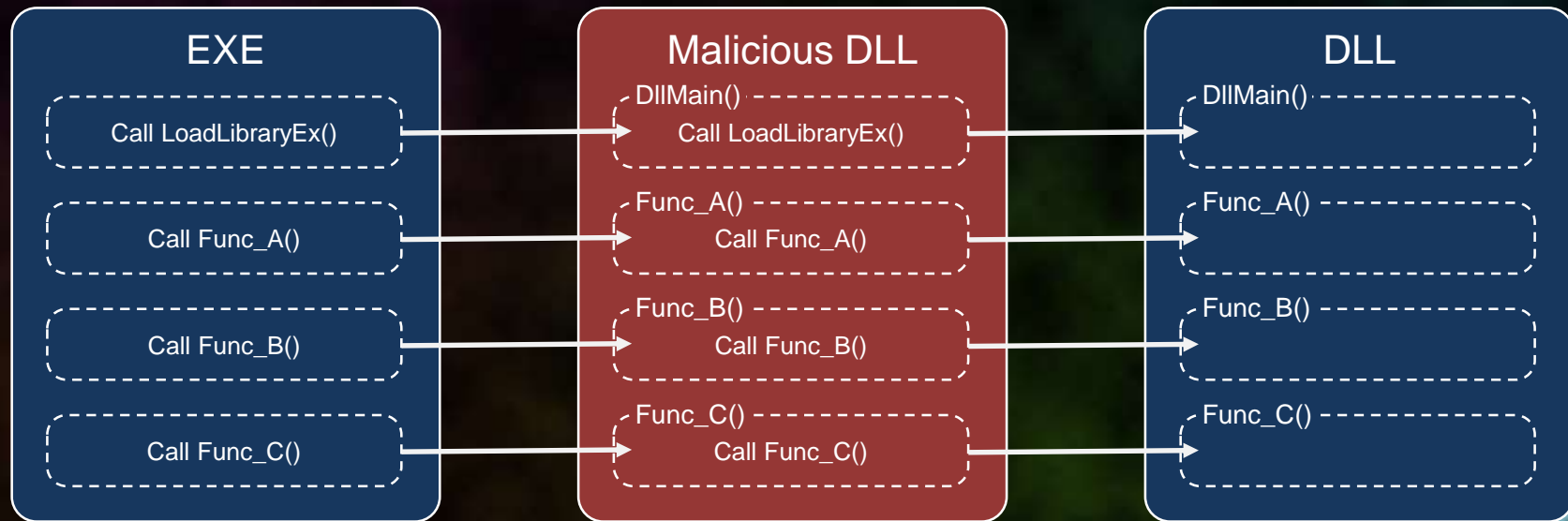
```
File Type: DLL
Section contains the following exports for 1Password.dll

00000000 characteristics
FFFFFFFF time date stamp
0.00 version
1 ordinal base
156 number of functions
156 number of names

ordinal hint RVA      name
1 0 001820F0 WorkspaceDrop
2 1 001820C0 WorkspaceNew
3 2 00182F80 WorkspaceUnlock
4 3 00192430 backup_local_vault
5 4 0019B150 bool_policy
6 5 00194E00 brain_log
7 6 00358EF0 bz_internal_error
8 7 00004770 call
9 8 00192470 can_backup_local_vault
10 9 0019C400 clear_proxy
11 A 0018E860 count_accounts
12 B 00186A30 count_offline_changes
13 C 0019D170 create_http_response
14 D 00186D50 create_item
15 E 0019A580 create_item_details_json
```

Can steal the information of Functions

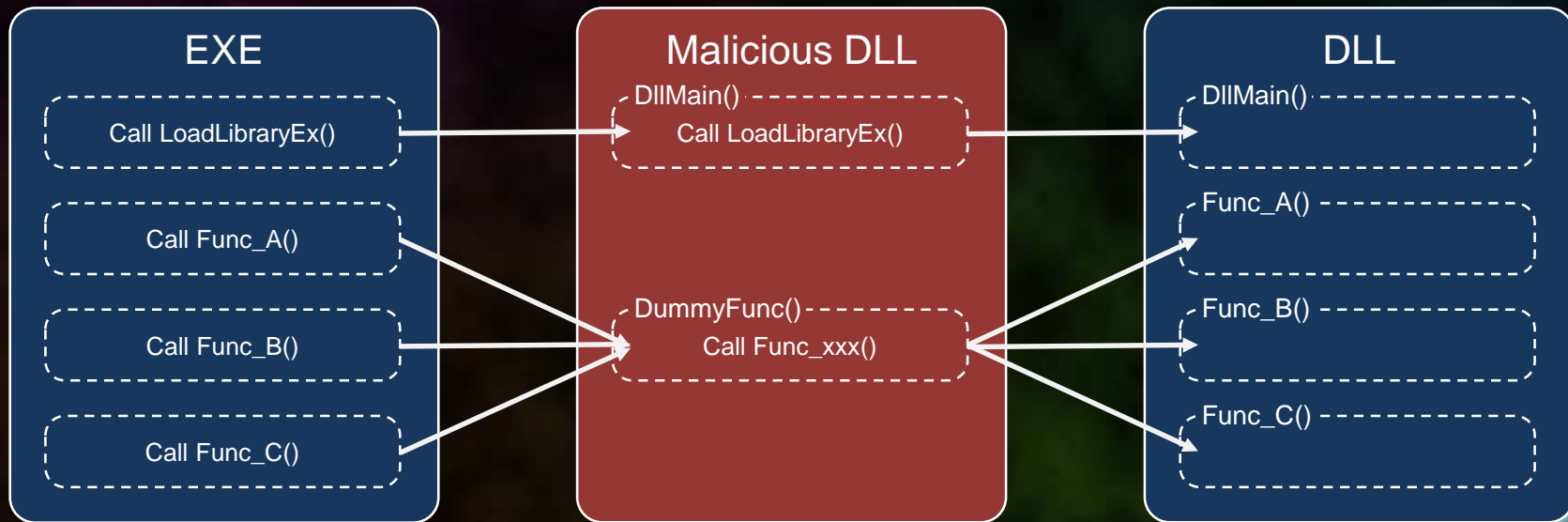
Implementation of all functions is impossible



Need a generic DLL

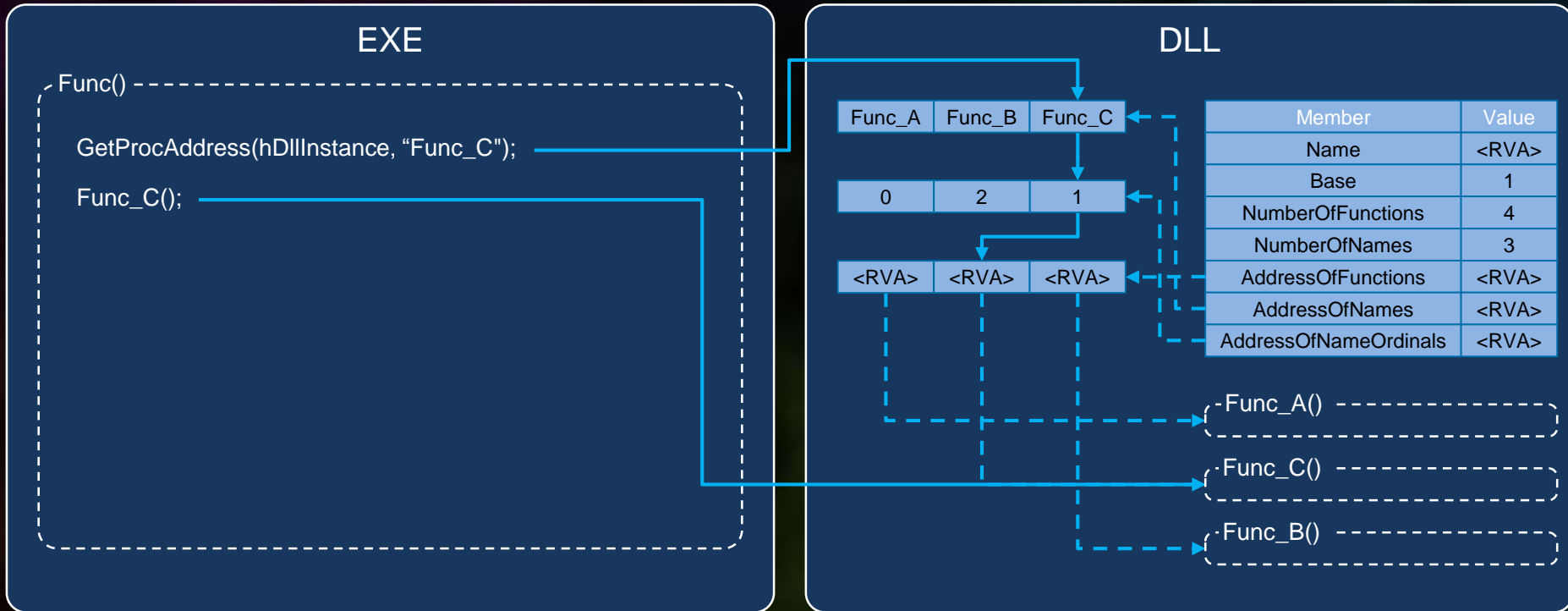
Does not depend on

- number of export functions
- number of arguments



Generate export table dynamically

Exe gets address of function via GetProcAddress



Generate export table dynamically

Copy export table from correct dll

Malicious DLL

Func_A Func_B Func_C

0 2 1

<RVA> <RVA> <RVA>

Name	<RVA>
Base	1
NumberOfFunctions	4
NumberOfNames	3
AddressOfFunctions	<RVA>
AddressOfNames	<RVA>
AddressOfNameOrdinals	<RVA>

Func[0]	Func[1]	Func[2]
0xFFFF	0xFFFF	0xFFFF

```
DummyFunc()
0xFFFFFFFF movzx eax, word ptr[n]
0xFFFFFFFF inc ax
0xFFFFFFFF mov word ptr[n], ax
0xFFFFFFFF movzx eax, word ptr[n]
0xFFFFFFFF inc ax
0xFFFFFFFF mov word ptr[n], ax
0xFFFFFFFF JMP Func[n]
```

DLL

Func_A Func_B Func_C

0 2 1

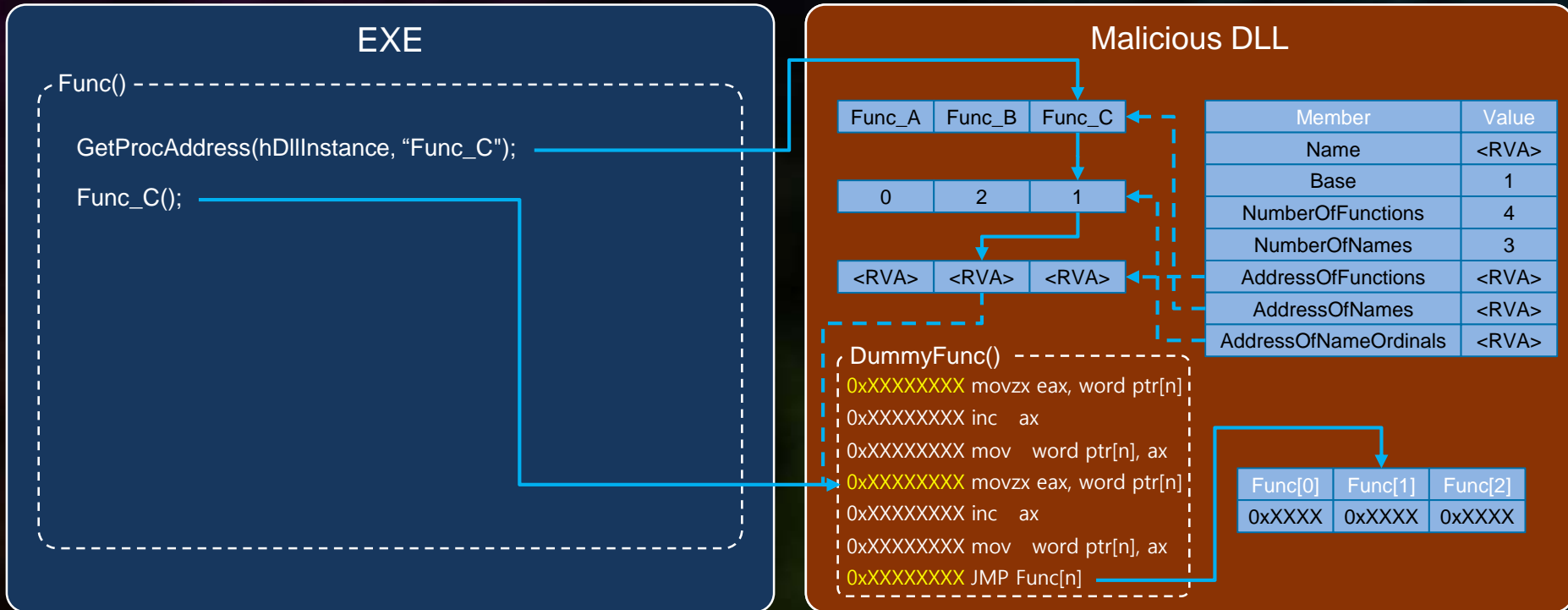
<RVA> <RVA> <RVA>

Member	Value
Name	<RVA>
Base	1
NumberOfFunctions	4
NumberOfNames	3
AddressOfFunctions	<RVA>
AddressOfNames	<RVA>
AddressOfNameOrdinals	<RVA>

Func_A() ---
Func_C() ---
Func_B() ---

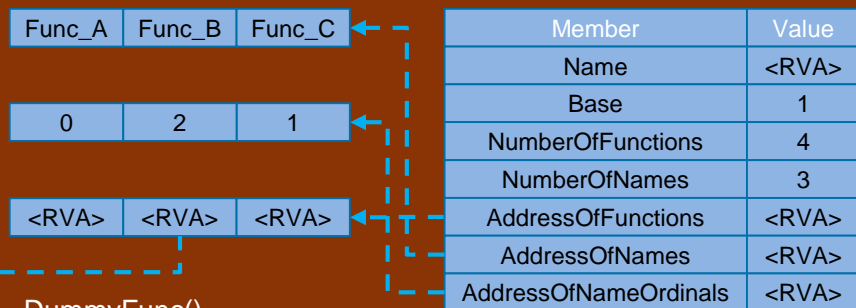
Generate export table dynamically

Exe gets incorrect address from malicious dll



Generate export table dynamically

Malicious DLL



DummyFunc() -

0xFFFFFFFF movzx eax, word ptr[n]

0xFFFFFFFF inc ax

0xFFFFFFFF mov word ptr[n], ax

0xFFFFFFFF movzx eax, word ptr[n]

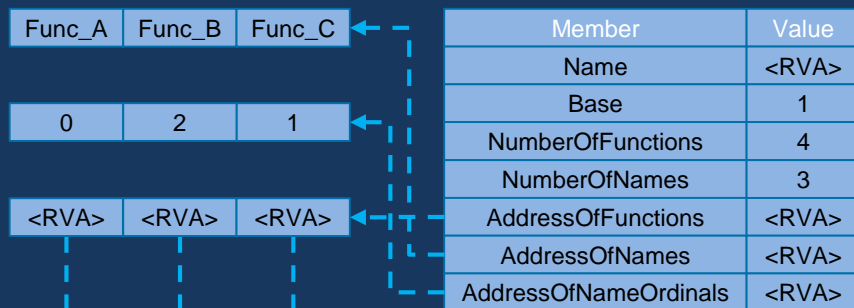
0xFFFFFFFF inc ax

0xFFFFFFFF mov word ptr[n], ax

0xFFFFFFFF JMP Func[n]

Func[0]	Func[1]	Func[2]
0xFFFF	0xFFFF	0xFFFF

DLL



Func_A()

Func_C()

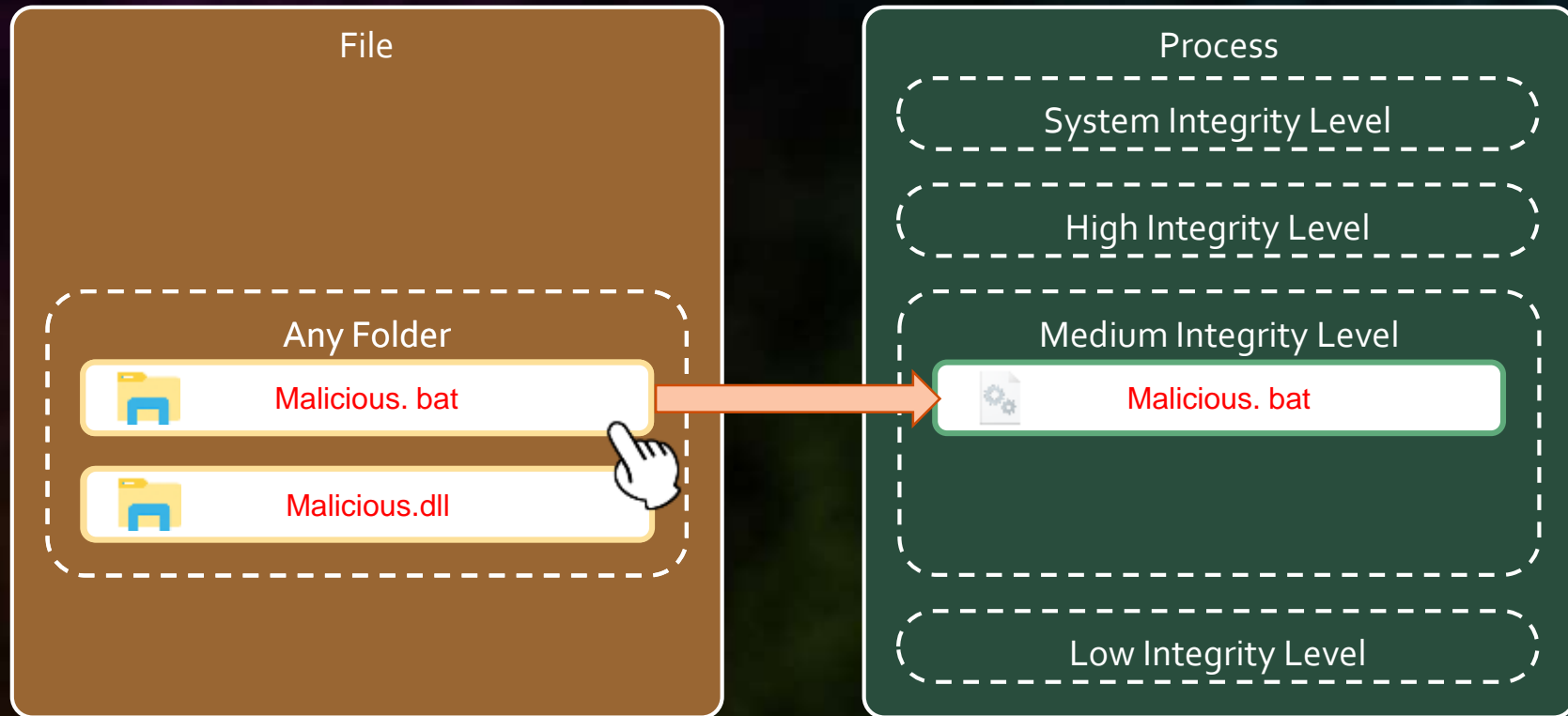
Func_B()

Demonstration video 3



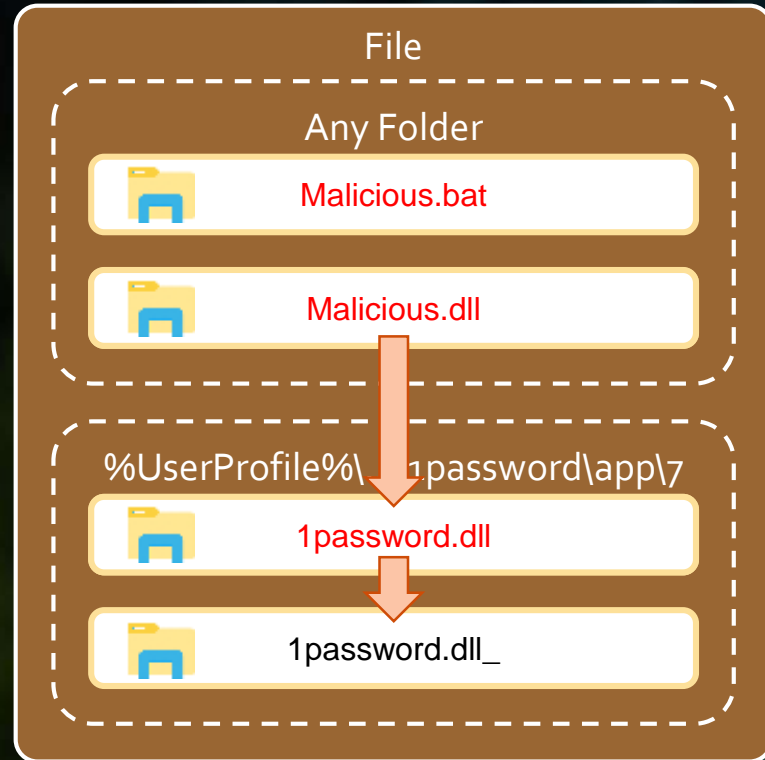
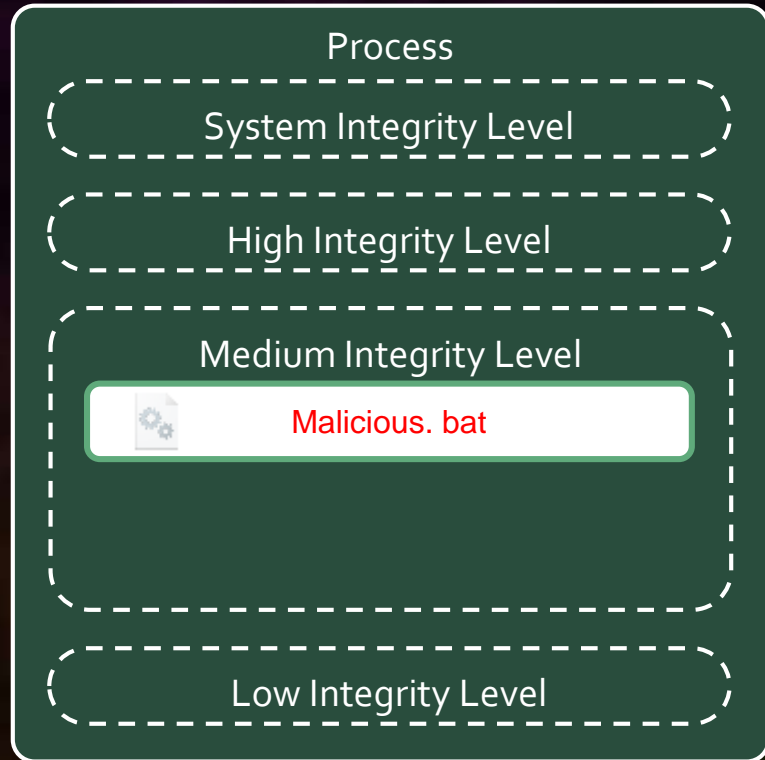
Mechanism

User executes malicious program



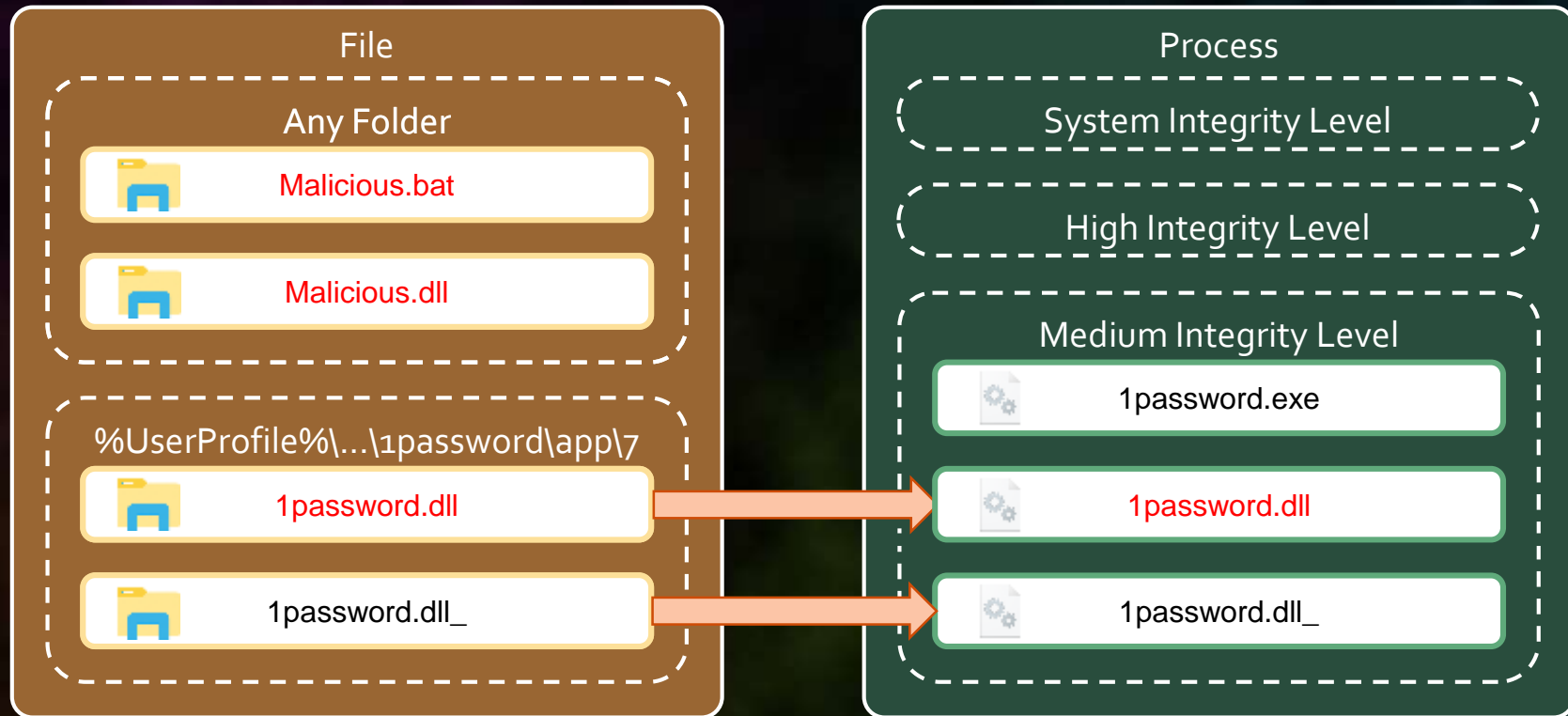
Mechanism

Malicious program replaces correct dll with itself



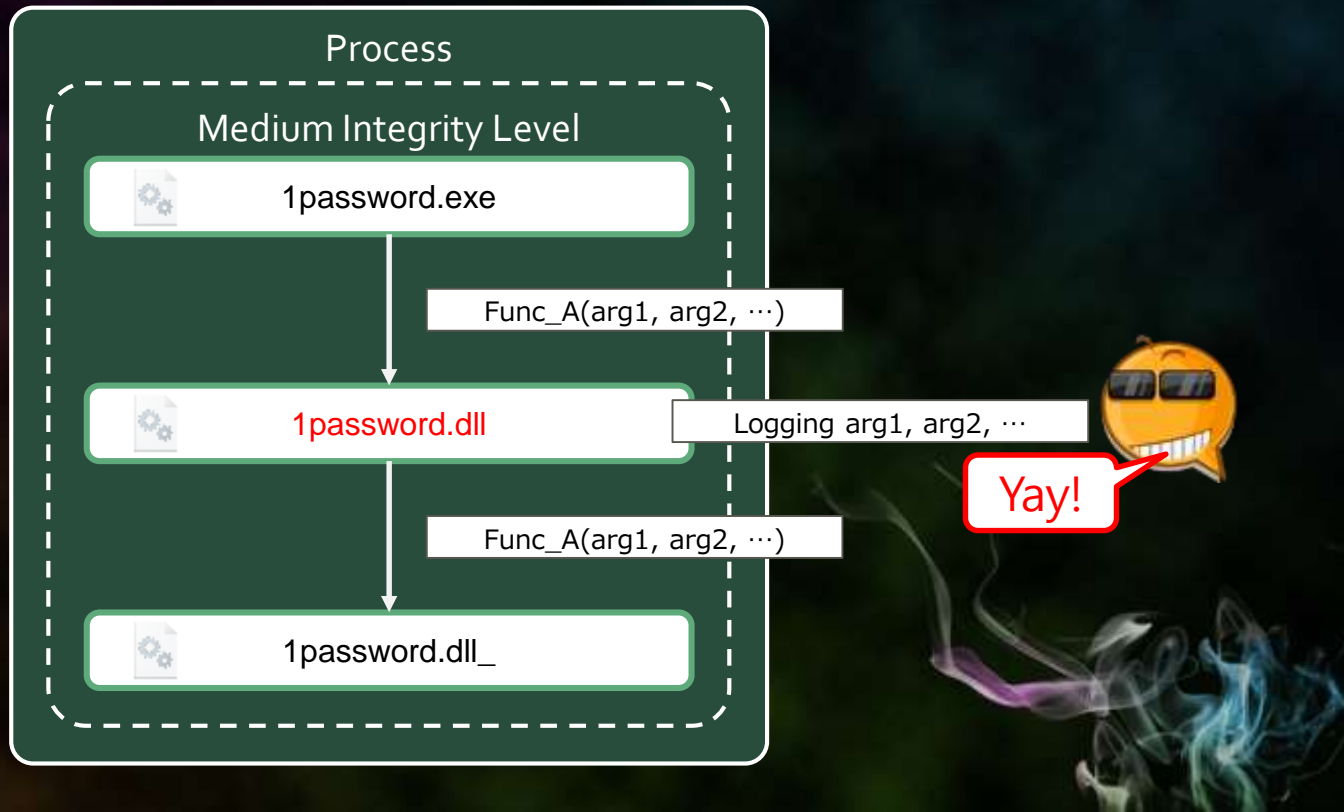
Mechanism

1Password loads malicious dll



Mechanism

The information between exe to dll is plain text



Bug Bounty Program

[Who We Are](#)[Product](#)[Resources](#)[Customers](#)[Programs](#)[About](#)[Learn More](#)

1Password

1Password is the world's best password manager. Perfect for protecting your business, team, and family.

🚩 **Points – \$5,000 per vulnerability** ⭐ **Up to \$100,000 maximum reward**

🏷️ Managed by Bugcrowd

[SUBMIT REPORT](#)[Program details](#)[Program updates](#) 8[Hall of Fame](#)[Tweet](#)[Share 34](#)

**It's revenge again
I submitted a vulnerability report
1Pssword said...**



1Password said... can **not** pay the reward



trim_bugcrowd added a comment

23 Mar 2019 01:14:26 JST

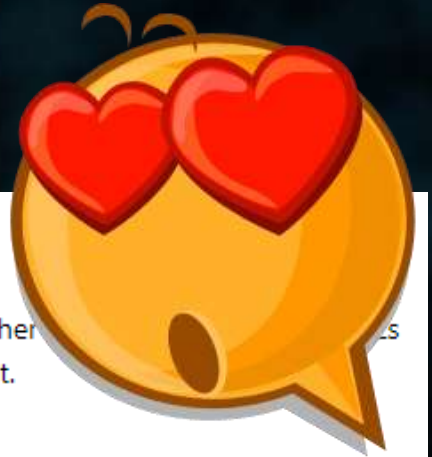
Hi SoyaAoyama,

We appreciate your work on this submission. This issue was reported before by other researchers as well. However, after this was reviewed along with 1Password team, **it does not qualify for a bounty** as it is an attack that depends on a compromise of the user's operating system and environment. That is actually considered as out of scope on this program. As you reported this once on the other program, I am closing it as N/A this time.

Best regards,

- trim_bugcrowd

However, after 3 hours pay the reward



Jeffrey_Goldberg rewarded **SoyaAoyama** \$100

23 Mar 2019 04:36:53 JST

As noted earlier, we can't defend against local compromises, but we are looking at ways to further from. And so because your report resulted in actions and potential changes, we are rewarding it.



Jeffrey_Goldberg rewarded **SoyaAoyama** \$400

23 Mar 2019 04:39:08 JST

Although local attacks are out of scope, I wanted to add a bonus as we are more systematically reviewing what practically can be done.

1Password releases beta version

7.3.701.BETA (build #701) – released 2019-07-05 – [download](#)

NEW

- Added support for an upcoming feature with 1Password memberships. Stay tuned for more details. {OPW-3904}

IMPROVEMENTS

- Added temporary support for Opera 60 stable version with an expired key within a valid certificate. {OPW-4001}
- 1Password will notify if an attempt to run 1Password with administrator rights is made. Instead, run 1Password normally and it'll request it when needed. {OPW-3775}

SECURITY

- 1Password will now require administrator rights to install and to update. Thanks to @SoyaAoyama for his reports. {OPW-3959, OPW-3887}
- Inform Windows to limit our DLL search to the 1Password's app directory only and not look for it elsewhere in the default list of known locations. Thanks to @SoyaAoyama for his reports. {OPW-3833}
- Added 1Password.brain.exe to be opt'd out of Windows Error Reporting. {OPW-3804}
- Removed the --database-path support from 1Password.exe as it could be abused to redirect 1Password to an unexpected location. We recommend using Group Policy to set the database path instead. Thanks @zemnmez! {OPW-3776, OPW-3778}

I just want to say one word!!

Only \$500?



security impact

Used by over 40,000 businesses with hundreds of glowing reviews

The New York Times

CNN

npr

TE

theguardian

- Does not require administrator privileges
- Remote impersonation is possible

Why is local hacking neglected?

- Because, you got already hacked.

**Are there nothing to consider
after such an invasion?**



In Local

- A lot of important data
- Many things attackers can do without becoming administrator

You would take local hacking after intrusion into account



@SoyaAoyama



<https://www.facebook.com/soya.aoyama.3>



<https://www.slideshare.net/SoyaAoyama>