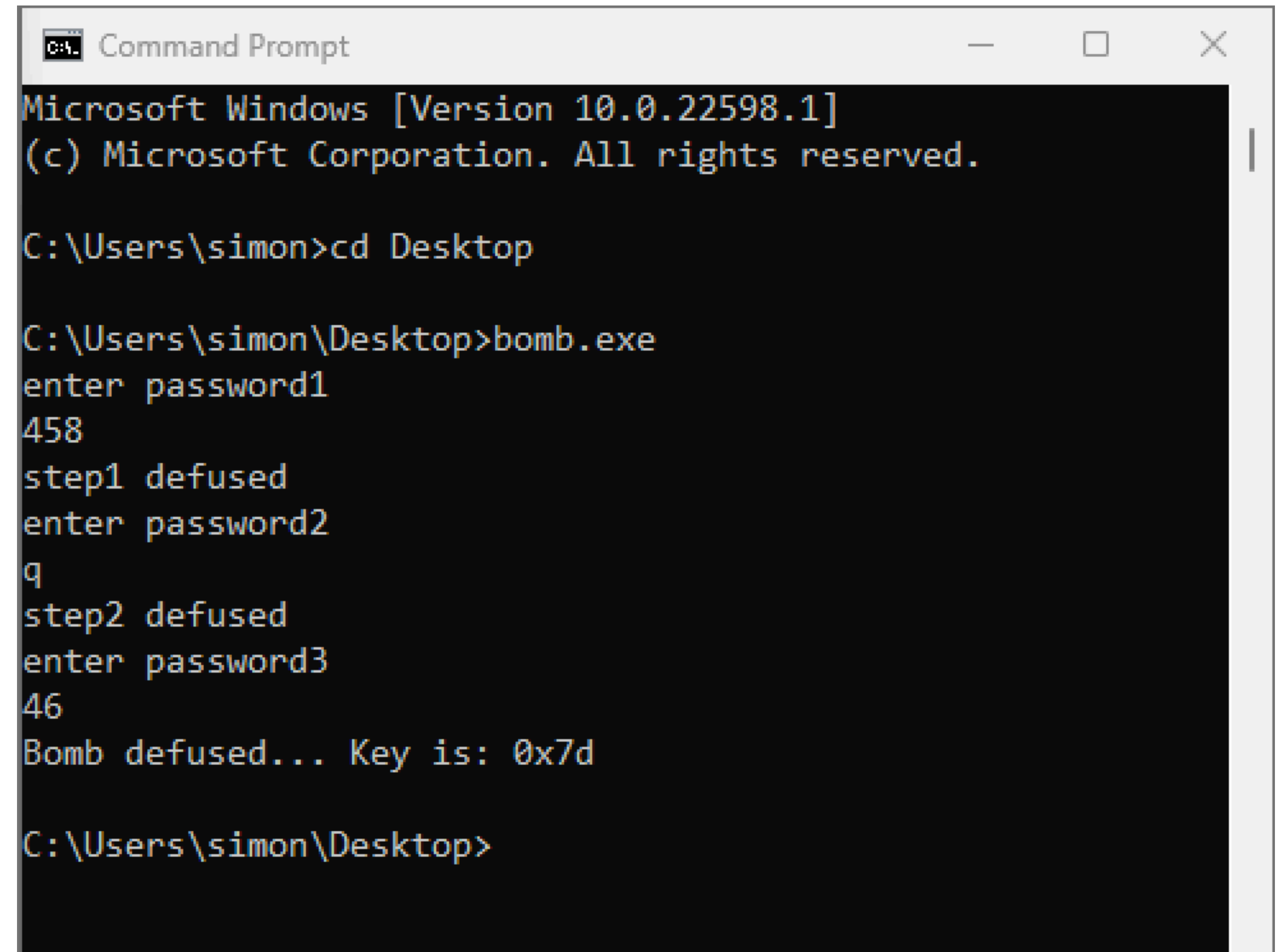


bomb.exe analysis

using ida64

Setup

- Password: “infected”
- Command-line program
- Must enter 3 passwords
- Wrong password \Rightarrow it “explodes”
- Final key is derived from input
- No bypassing



```
Command Prompt
Microsoft Windows [Version 10.0.22598.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\simon>cd Desktop

C:\Users\simon\Desktop>bomb.exe
enter password1
458
step1 defused
enter password2
q
step2 defused
enter password3
46
Bomb defused... Key is: 0x7d

C:\Users\simon\Desktop>
```

First defuse step

<pre>; Attributes: bp-based frame fuzzy-sp ; int __cdecl main(int argc, const char **argv, const char **envp) public _main _main proc near var_18= dword ptr -18h var_11= byte ptr -11h var_10= dword ptr -10h var_C= dword ptr -0Ch var_4= dword ptr -4 argc= dword ptr 8 argv= dword ptr 0Ch envp= dword ptr 10h</pre>		Define variables
<pre>; __unwind { lea ecx, [esp+4] and esp, 0FFFFFFF0h push dword ptr [ecx-4] push ebp mov ebp, esp push ecx sub esp, 24h call __main</pre>		"Stuff"
<pre>mov dword ptr [esp+4], offset aEnterPassword1 ; "enter password1" mov dword ptr [esp], offset __imp__ZSt4cout ; std::cout call __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::char_traits<char>>(std::basic_ost mov dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_ ; std::endl<char,std::char_tr mov ecx, eax call __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*) (std::ostream &)) sub esp, 4 lea eax, [ebp+var_10] mov [esp], eax</pre>		Print prompt to std::cout
<pre>mov ecx, offset __imp__ZSt3cin ; std::cin call __ZNSirsERi ; std::istream::operator>>(int &) sub esp, 4</pre>		Read int from std::cin
<pre>mov eax, [ebp+var_10] cmp eax, 1CAh</pre>		Compare 0x1CA (458) with input
<pre>jnz loc_401645</pre>		Jump if not equal

Failure



```
loc_401645:
mov     dword ptr [esp+4], offset aBombExploded ; "bomb exploded"
mov     dword ptr [esp], offset __imp__ZSt4cout ; std::cout
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; s
mov     dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13
mov     ecx, eax
call    __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream &
sub     esp, 4
```

Print message to std::cout

Second defuse step

<pre>mov dword ptr [esp+4], offset aStep1Defused ; "step1 defused" mov dword ptr [esp], offset __imp__ZSt4cout ; std::cout call __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<< mov dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_c mov ecx, eax call __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*)(&std sub esp, 4</pre>	Print message to std::cout
<pre>mov dword ptr [esp+4], offset aEnterPassword2 ; "enter password2" mov dword ptr [esp], offset __imp__ZSt4cout ; std::cout call __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<< mov dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_c mov ecx, eax call __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*)(&std sub esp, 4</pre>	Print prompt to std::cout
<pre>lea eax, [ebp+var_11] mov [esp+4], eax mov dword ptr [esp], offset __imp__ZSt3cin ; std::cin call __ZStrsIcSt11char_traitsIcEERSt13basic_istreamIT_T0_ES6_RS3_ ; std:: movzx eax, [ebp+var_11] cmp al, 71h ; 'q' jnz loc_40161E</pre>	Read char from std::cin Compare 0x71 ('q') to input Jump if not equal

Third defuse step

```
mov     dword ptr [esp+4], offset aStep2Defused ; "step2 defused"
mov     dword ptr [esp], offset __imp__ZSt4cout ; std::cout
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std: Print message to std::cout
mov     dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_
mov     ecx, eax
call    __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*) (std::ostream &
sub     esp, 4
mov     dword ptr [esp+4], offset aEnterPassword3 ; "enter password3"
mov     dword ptr [esp], offset __imp__ZSt4cout ; std::cout
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std: Print prompt to std::cout
mov     dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_
mov     ecx, eax
call    __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*) (std::ostream &
sub     esp, 4
lea     eax, [ebp+var_18]
mov     [esp], eax
mov     ecx, offset __imp__ZSt3cin ; std::cin Read int from std::cin
call    __ZNSirsERi ; std::istream::operator>>(int &)
sub     esp, 4
mov     [ebp+var_C], 0Dh ; move 13 into var_c
add     [ebp+var_C], 0Ah ; add 10 to var_c "Construct" 46 in var_C
shl     [ebp+var_C], 1 ; shift left once, i.e. multiply by 2
mov     eax, [ebp+var_18] ; move stdin to eax
cmp     eax, [ebp+var_C] ; compare with var_c Compare var_c to input
jnz     short loc_4015F7 ; jump if not zer / jump if not equal Jump if not equal
```

Success

```
xor     [ebp+var_C], 53h
mov     dword ptr [esp+4], offset aBombDefusedKey ; "Bomb defused... Key is: "
mov     dword ptr [esp], offset __imp__ZSt4cout ; std::cout           Print message to std::cout
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std
mov     dword ptr [esp], offset __ZSt8showbaseRSt8ios_base ; std::showbase(std::ios_base
mov     ecx, eax
call    __ZNSolsEPFRSt8ios_baseS0_E ; std::ostream::operator<<(std::ios_base & (*)(std
sub     esp, 4
mov     dword ptr [esp], offset __ZSt3hexRSt8ios_base ; std::hex(std::ios_base &)
mov     ecx, eax
call    __ZNSolsEPFRSt8ios_baseS0_E ; std::ostream::operator<<(std::ios_base & (*)(std
sub     esp, 4
mov     edx, eax
mov     eax, [ebp+var_C]           "Stuff" to construct key
mov     [esp], eax
mov     ecx, edx
call    __ZNSolsEi ; std::ostream::operator<<(int)
sub     esp, 4
mov     dword ptr [esp], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_T6
mov     ecx, eax
call    __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*)(std::ostream &
sub     esp, 4
jmp     short loc_40166A           Jump to end
```

