TEAMT5
杜 浦 數 位 安 全

Japan Security Analyst Conference 2020

Evil Hidden in Shellcode:
The Evolution of Malware DBGPRINT

Malware Researcher

CiYi "YCY" Yu
Aragorn Tseng

Malware Researcher!

TEAMT5
杜浦數位安全

CiYi "YCY" Yu

1P

Malware Analysis
Campaign Tracking
Automated Analysis

Aragorn Tseng

2P

Malware analysis
Incident response
Machine learning

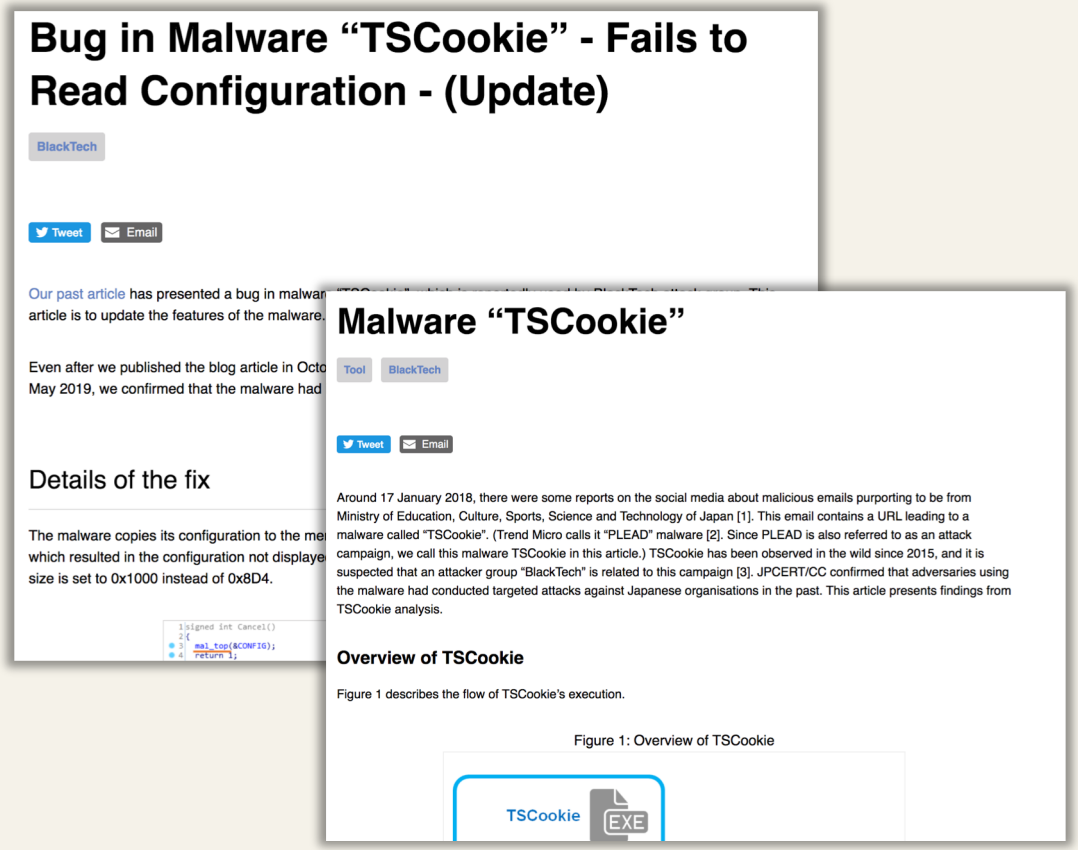
AGENDA

- Adversary Profile: HUAPI
- Malware Profile: DBGPRINT
- Evolution of DBGPRINT
- In-Depth Analysis of DBGPRINT
- Detection Warfare
- Remediation & Detection

TEAMT5
杜 浦 數 位 安 全

Adversary Profile: HUAPI

- Alias BlackTech
- Since 2007
- Malware:
  - TSCOOKIE
  - KIVARS
  - CAPGELD
  - DBGPRINT



Bug in Malware “TSCookie” - Fails to Read Configuration - (Update)

BlackTech

Tweet Email

Our past article has presented a bug in malwar
article is to update the features of the malware.

Even after we published the blog article in Octo
May 2019, we confirmed that the malware had

Details of the fix

The malware copies its configuration to the me
which resulted in the configuration not displaye
size is set to 0x1000 instead of 0x8D4.

```
signed int Cancel()
{
  mal_top(&CONFIG);
  return 1;
}
```

Malware “TSCookie”

Tool BlackTech

Tweet Email

Around 17 January 2018, there were some reports on the social media about malicious emails purporting to be from Ministry of Education, Culture, Sports, Science and Technology of Japan [1]. This email contains a URL leading to a malware called “TSCookie”. (Trend Micro calls it “PLEAD” malware [2]. Since PLEAD is also referred to as an attack campaign, we call this malware TSCookie in this article.) TSCookie has been observed in the wild since 2015, and it is suspected that an attacker group “BlackTech” is related to this campaign [3]. JPCERT/CC confirmed that adversaries using the malware had conducted targeted attacks against Japanese organisations in the past. This article presents findings from TSCookie analysis.

Overview of TSCookie

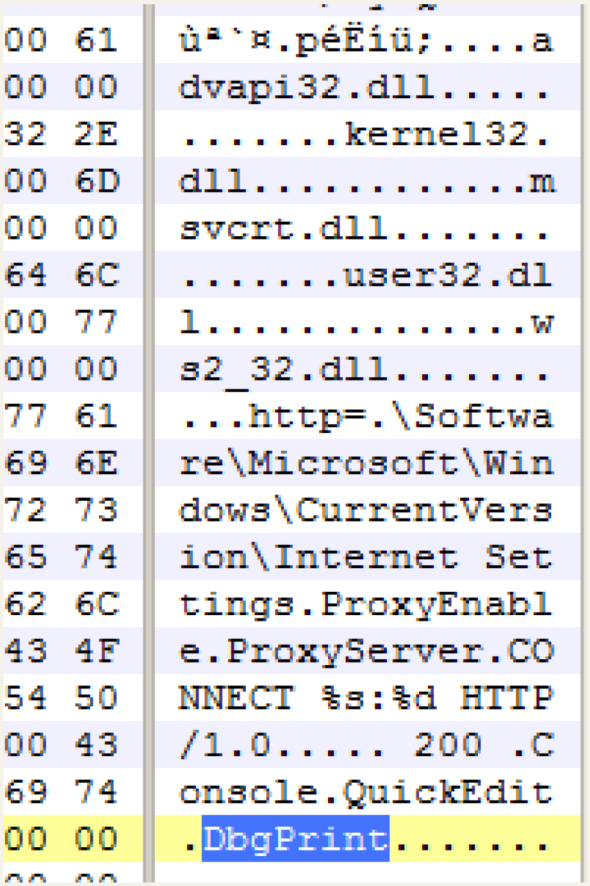
Figure 1 describes the flow of TSCookie’s execution.

Figure 1: Overview of TSCookie

TSCookie EXE

Malware Profile: DBGPRINT

- Alias Waterbear
- Since at least 2009
- DLL export name “DbgPrint”
- Acted as second stage
- Advanced malware design
  - Adopt shellcode stager
  - Able to load the plugins



Malware Profile: DBGPRINT

Government

Education

Think Tank

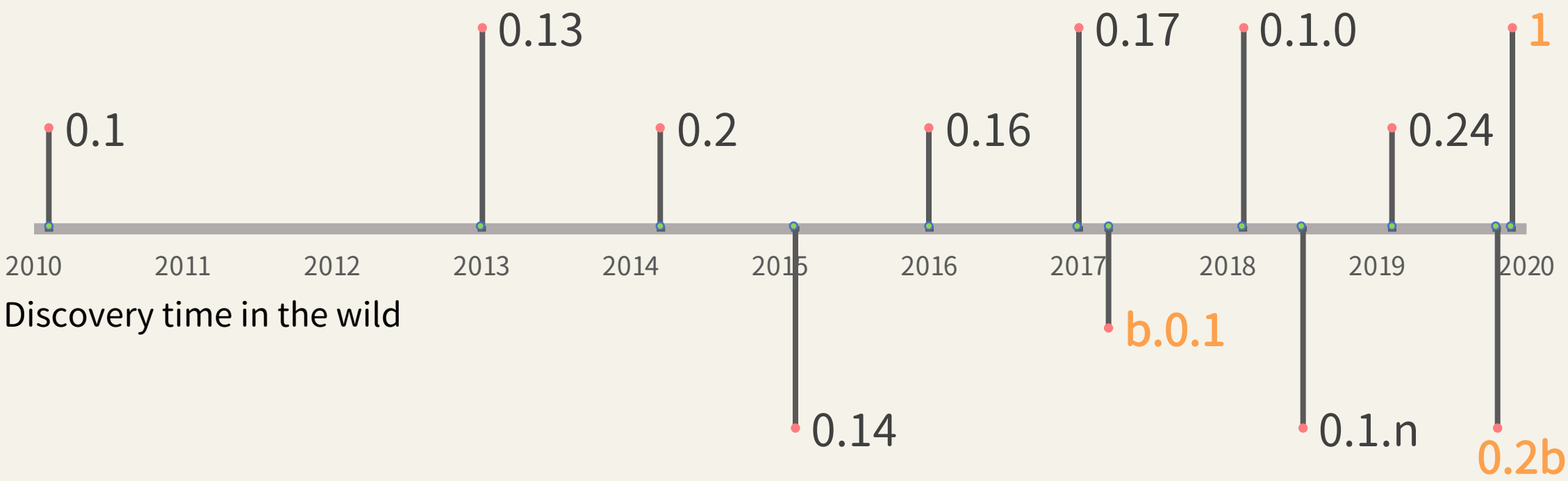
Finance

Technology

Healthcare

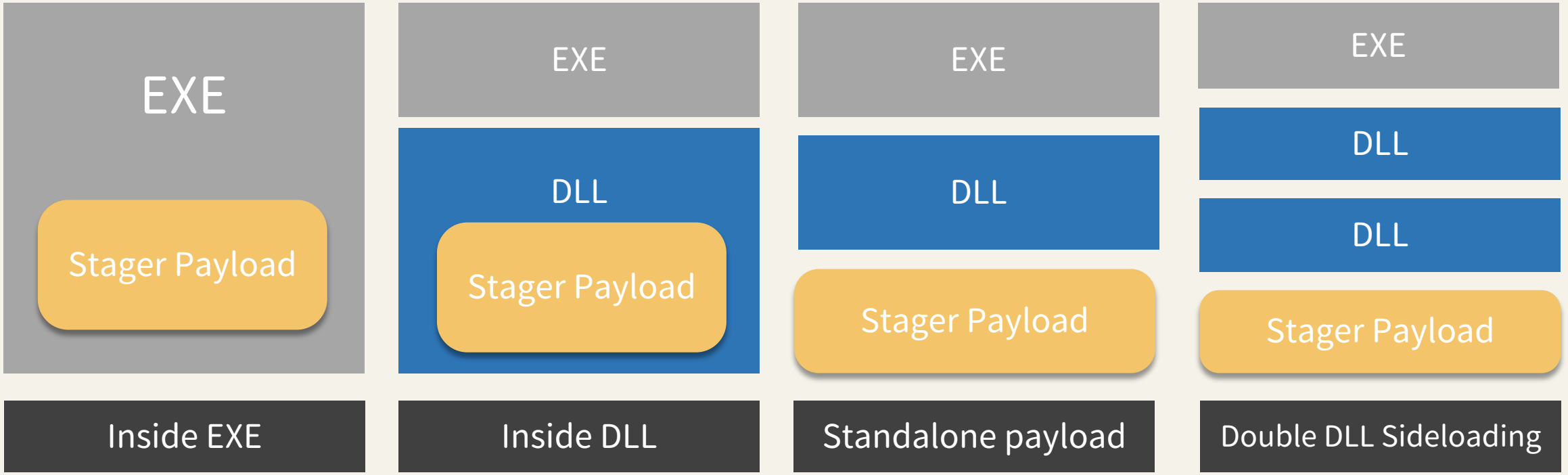
Evolution of DBGPRINT

Version Changes in the Wild



- Listen port —

Access Payload



RC4 Key of Payload

```
mov al, byte ptr [ecx]
mov dl, al
shr dl, 3
shl al, 5
or dl, al
mov byte ptr [ecx], dl
inc ecx
dec esi
jnz short 100010CD
```

XOR / Shift

01	03	FF	89
13	72	D1	0A
40	C0	21	BB

Random 16 bytes

C:\Program Files\NVIDIA Corporation\Display\nvwss.ptn\x00

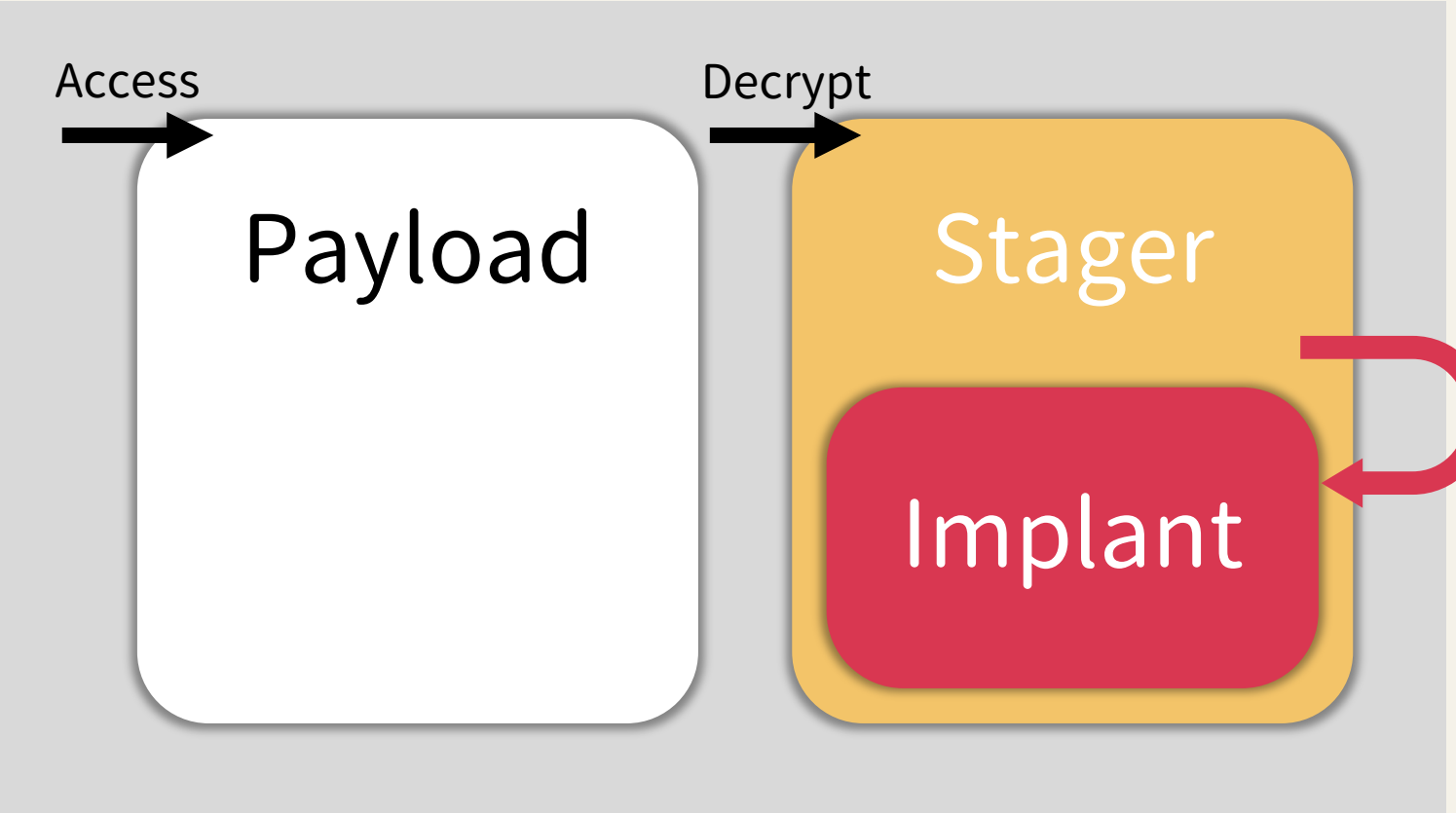
File path

Miss You! printupg.PNF

String + File name

In-Depth Analysis of DBGPRINT

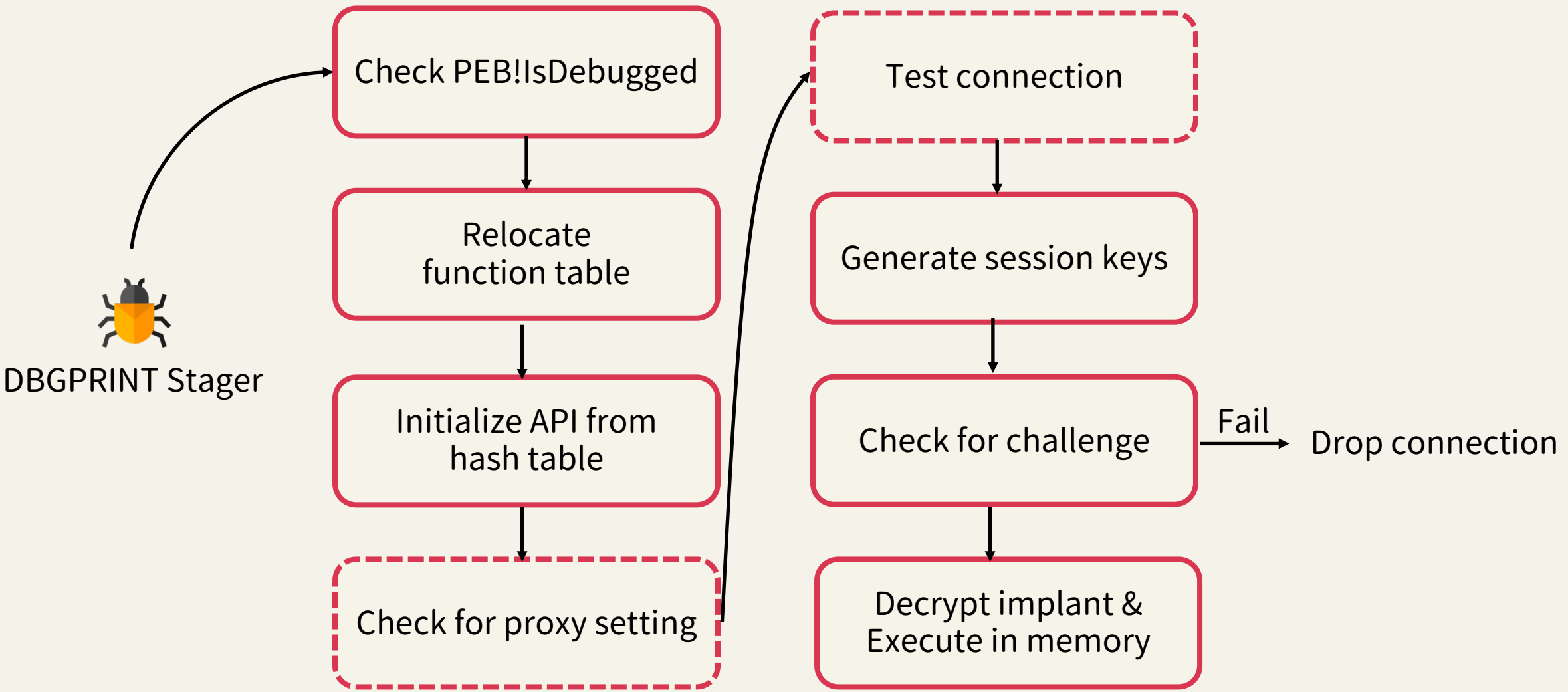
Execution Procedure



DBGPRINT Controller

1. Ask for DLL implant
2. Wait for connection

Inside DBGPRINT Stager



Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Generate request packet

Request the DBGPRINT implant with session keys

Calculate the pre-session key and challenge

Check for challenge

Send the calculated challenge

Decrypt implant and execute in memory

Send the DBGPRINT implant

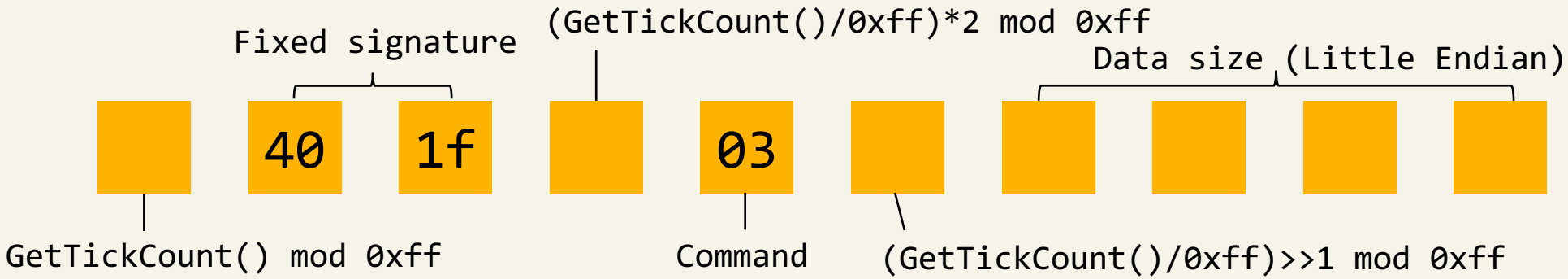
Split implant into encrypted blocks

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Generate request packet – Generate header



Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Generate request packet – Generate session keys

Authentication key ⊕ Random number = Pre-session key

Pre-session key ⊕ 0x6162636465666768696A6B6C6D6E6F00 = Session key 1

Pre-session key ⊕ 0x0102030405060708090001020304050 6 = Session key 2

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Generate request packet

Generate request packet

```
00000000  da 40 1f b5 03 6d 20 00  00 00
0000000A  35 c5 da 9c ae 62 04 f7  5a 36 29 19 b3 37 2d 45   Session key 1
0000001A  55 a5 ba fc ce 02 64 97  3a 5c 43 77 dd 5d 47 43   Session key 2
```

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Calculate the pre-session key and challenge

Session key 1 ⊕ 0x6162636465666768696A6B6C6D6E6F00 = Pre-session key

Pre-session key ⊕ Authentication key = Server challenge

Command for challenge

Server challenge

```
00000000  de 40 1f ee 01 bd 10 00  00 00 58 88 dc e1 84 f7
00000010  18 b2 50 8f 04 40 19 eb  47 a1
```

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Check for challenge

```
if (Server challenge ⊕ Pre-session key) == Authentication key:
        - Yes: Continue
        - No: Abort
```

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Split implant into encrypted blocks

```
# Modified_RC4_PRGA
for char in prga_data:
        x = (x + 1) % 256
        y = (y + box[x]) % 256
        box[x], box[y] = box[y], box[x]
        z = (box[x] + box[y]) % 256
        box[z] = ((box[z] << 4) & 0xf0) + ((box[z] >> 4) & 0x0f)
```

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Split implant into encrypted blocks

PRGA_data1 PRGA_data2 PRGA_data3

```
0000001A  90 15 8f 2a 96 e6 4e f8 91 ed 64 7c dc 46 47 30
0000002A  07 10 2c 6a 3d ac 47 e0 51 f7 86 02 07 2c 5e 0a
0000003A  44 b9 b6 f4 38 3d 63 79 b3 d1 53 58 b3 f1 10 ac
0000004A  95 35 52 17 f3 3b 1f ab 28 80 45 f2 c3 8c c2 d4
0000005A  a7 62 5a 76 48 25 8e 33 31 ba 33 b0 19 46 b0 17
…
…
…
```

PRGA_data4

Inside DBGPRINT Stager

DBGPRINT Stager

DBGPRINT Controller

Decrypt implant and execute in memory

```
RC4_KSA(Pre-session key)
decrypted data size header = RC4_PRGA(PRGA_data1)
decrypted data size = Modified_RC4_PRGA(PRGA_data2)
decrypted data header = Modified_RC4_PRGA(PRGA_data3)
decrypted data = Modified_RC4_PRGA(PRGA_data4)
```

DBGPRINT Implant

- File transfer / management

Command code	Capability
2	Enumerate disk drives
3	List files
4	Upload file to C2 server
5	Download file from C2 server
6	Rename file
7	Create folder
8	Delete file
10	Execute file
11	Move file
12	NtSetInformationFile

DBGPRINT Implant

- Windows management / Screenshot

Command code	Capability
807	Enumerate Windows
808	Hide Windows
809	Show Windows
810	Close Windows
811	Minimize Windows
812	Maximize Windows
814	Screenshot
815	Set screenshot event signaled

DBGPRINT Implant

- Remote desktop connection
- Process / Network connection / Service management

Command code	Capability
816	Remote desktop
817	Enumerate process
818	Terminate process
820	List network connection status
821	Abort a network connection
822	Enumerate services
827	Manipulate service

DBGPRINT Implant

- Remote shell / Registry management

Command code	Capability
1006	Start remote shell
1007	Exit remote shell
1008	Obtain remote shell PID
2011	Enumerate registry
2013	Create registry key
2014	Set registry key
2015	Delete registry key
2016	Delete registry value

Detection Warfare

Eliminate Patterns

```
1213141516......
èê..0.1.........
....Mutex.......
....login.narlla
b.com...........
................
................
................
................
................
............P.».
................
abcdefghijklmno.
./e.Oó{-cÓF5Ç².ä
```

Mutex

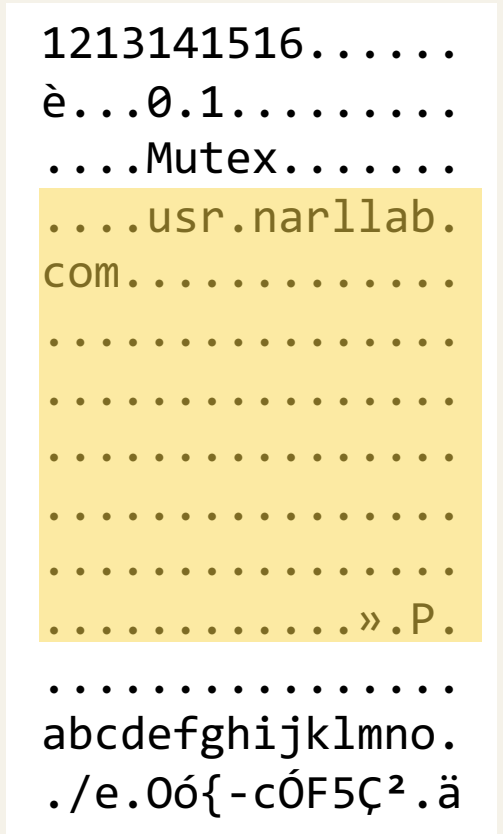
```
F.P...M...~...H1
....b.0.1.......
....M...........
................
................
................
................
................
................
................
................
................
........abcdefgh
ijklmno../e.O.{-
```

M

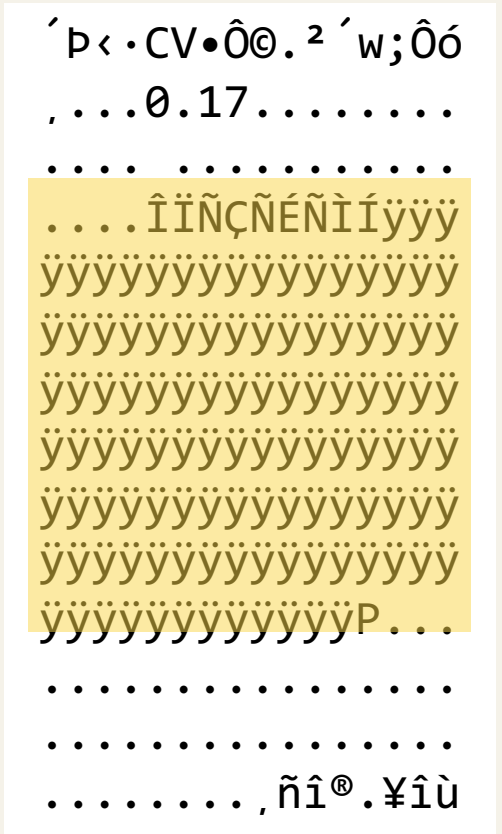
```
}8ºýáÈÒß¶î3ù.¿R–
,...0.24........
................
....ÎÏÑÍÏÑÎÎÈÑÎÎ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿ©a..
................
................
........q.ßä®;©ò
```

Space (0x20)

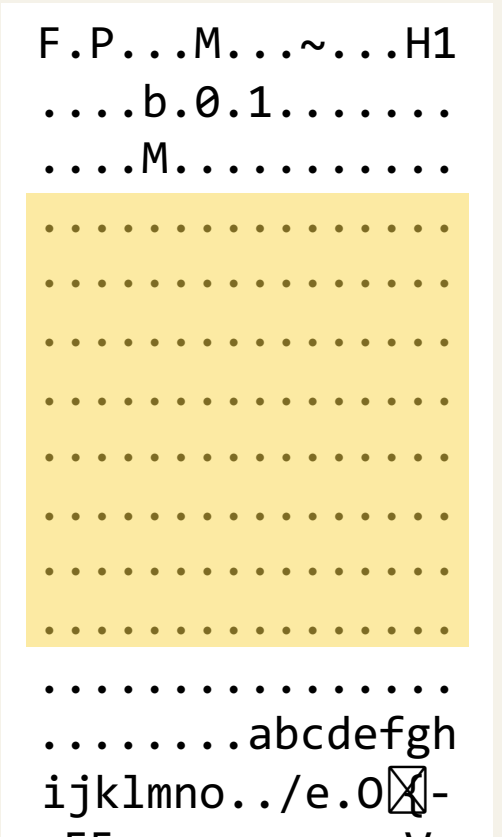
Eliminate Patterns



Plain text

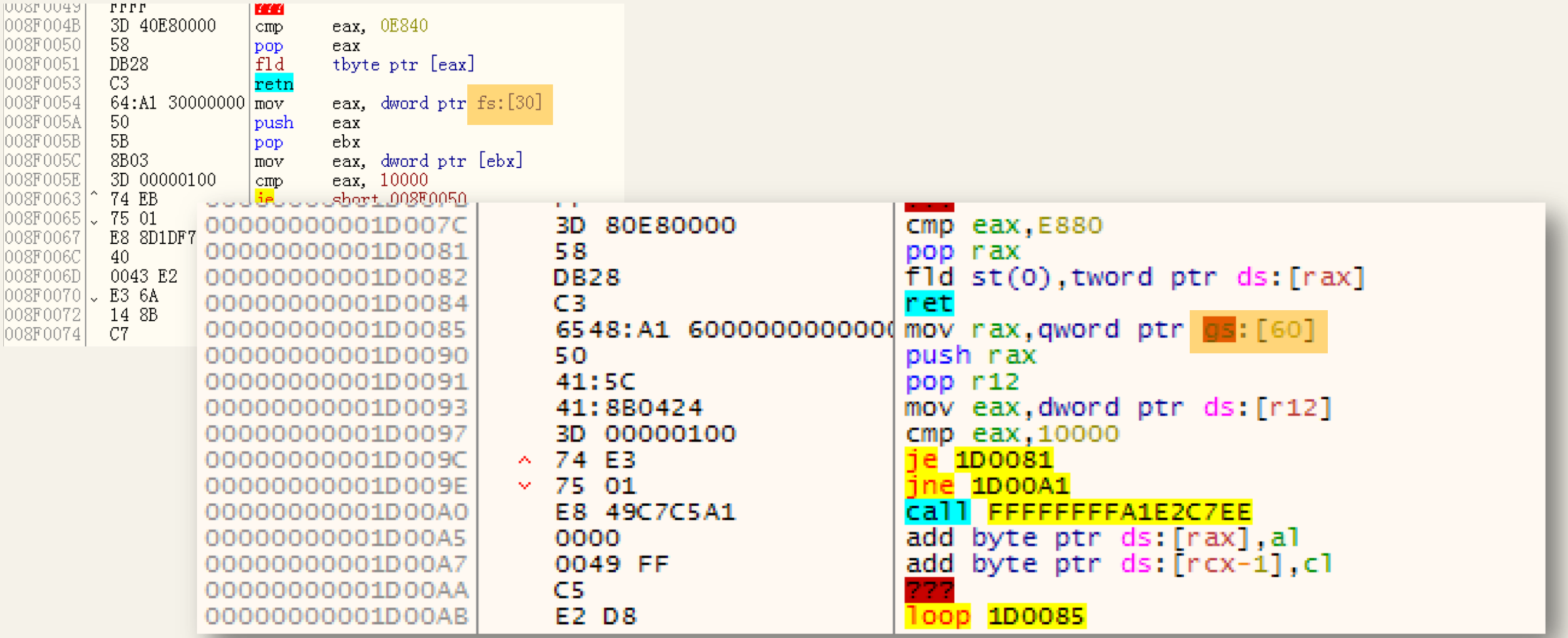


XOR with 0xff



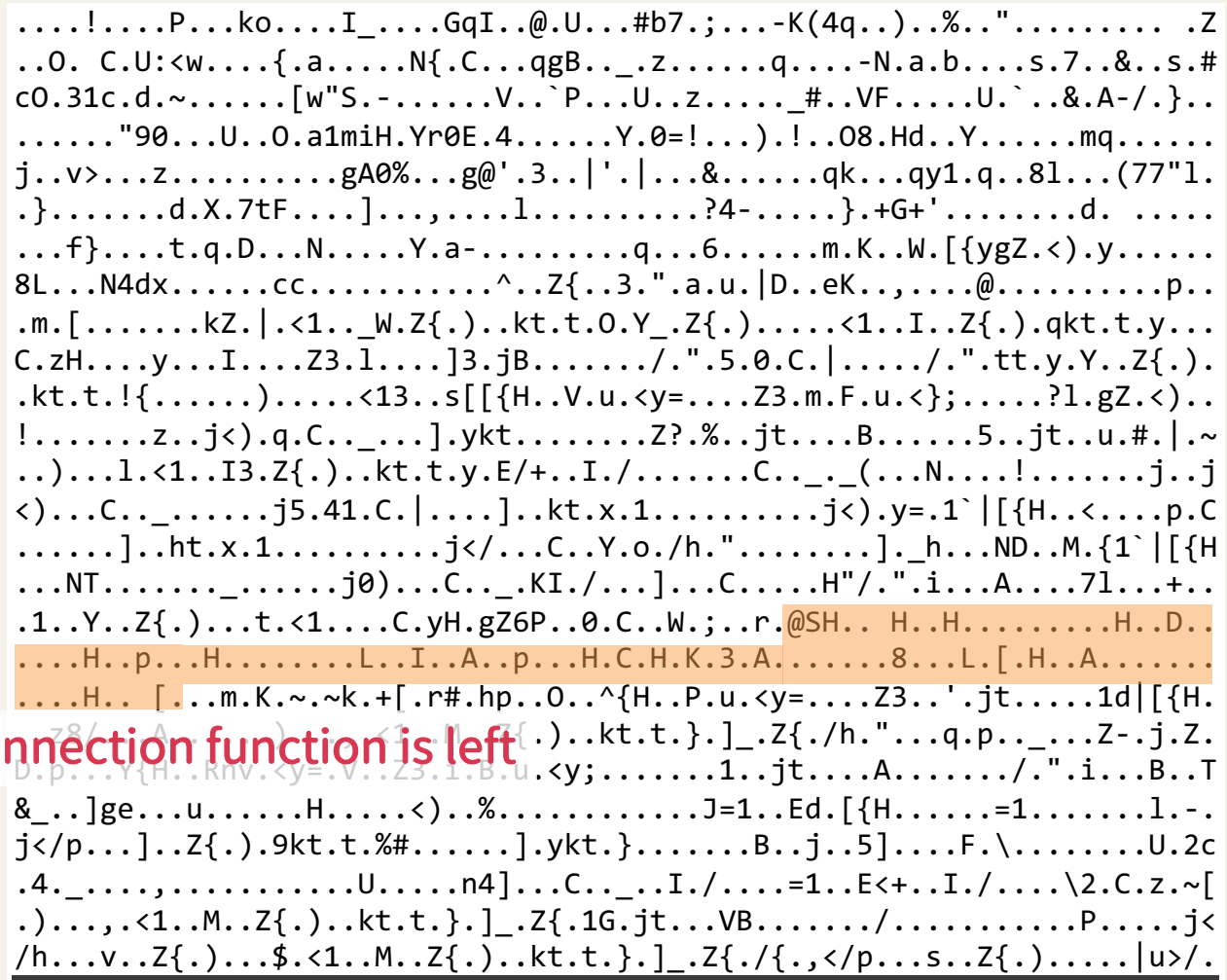
Listen port

x64 Version



Self-Modifying Code

Before self-modifying



After self-modifying

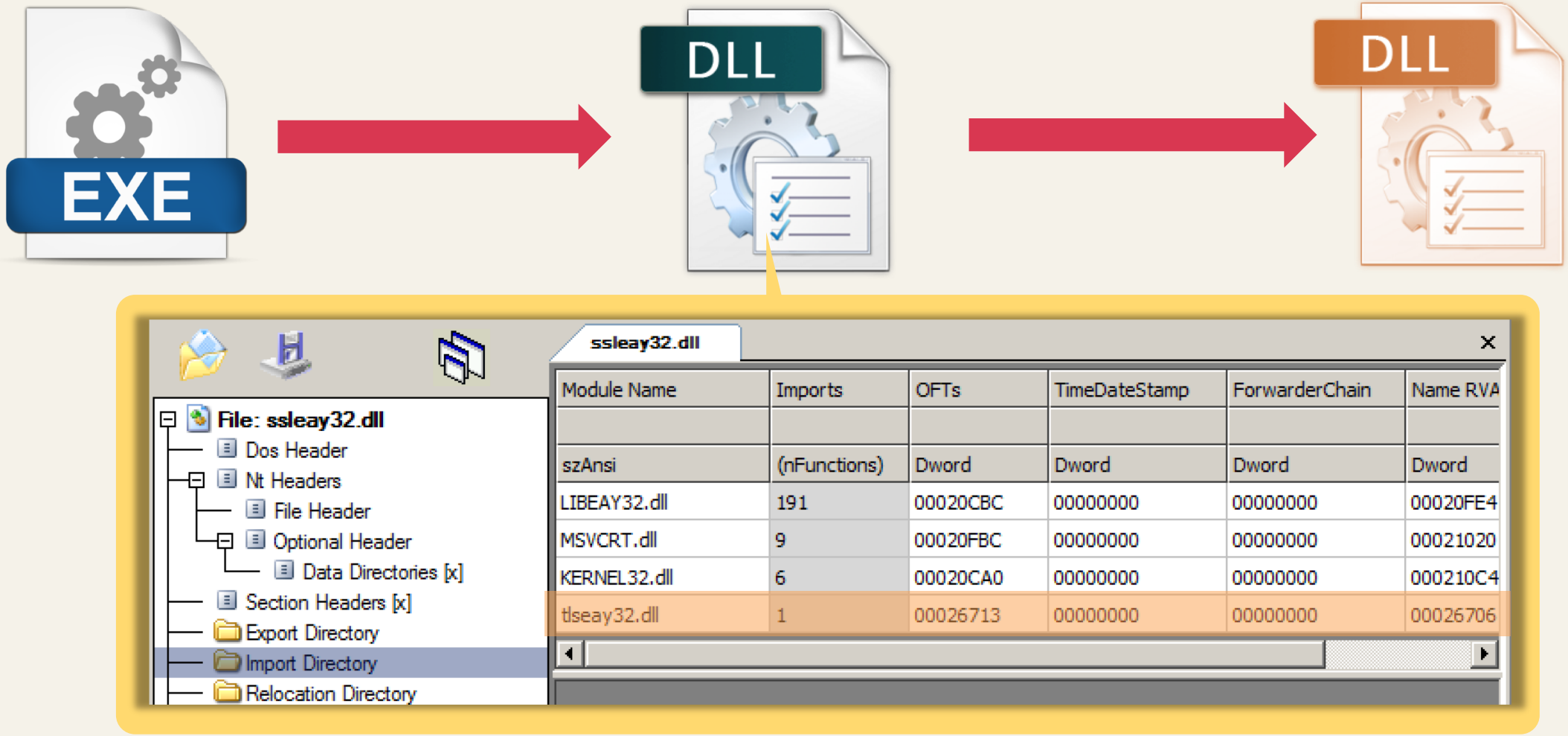
Only the wait-for-connection function is left

Double DLL Sideloading

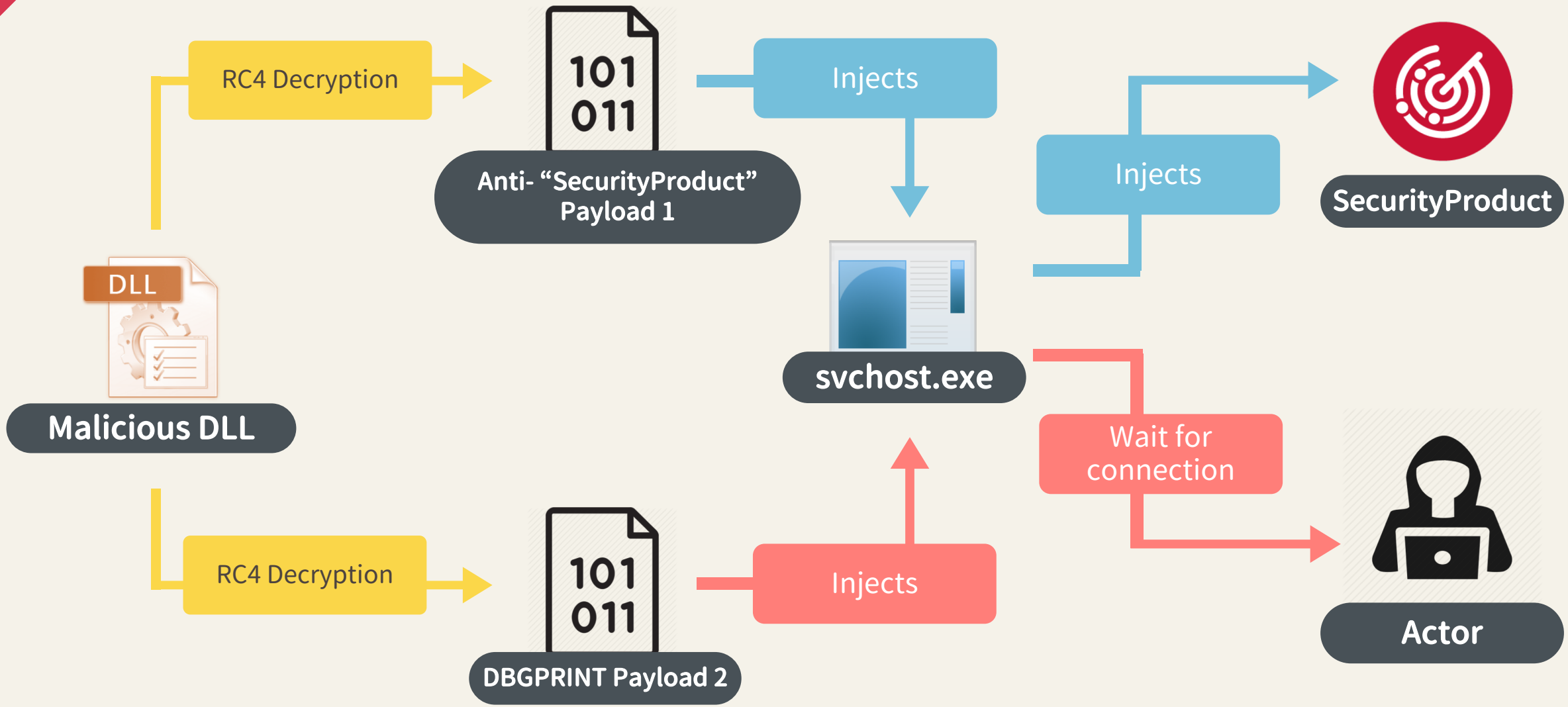
(White) Benign EXE

(Gray) Malicious DLL

(Black) Malicious DLL



Anti ”SecurityProduct”



Questions?

TEAMT5
杜 浦 數 位 安 全

ycy@teamt5.org
aragorn@teamt5.org