



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



TEAM5
杜通數位安全

Malware Researcher!



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



TEAM T5
杜浦數位安全

Adversary Profile: HUAPI



- ◆ Alias BlackTech
- ◆ Since 2007
- ◆ Malware:
 - ◆ TSCCOOKIE
 - ◆ KIVARS
 - ◆ CAPGELD
 - ◆ DBGPRINT

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

BlackTech

Tweet Email

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

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

Details of the fix

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

```
1 signed Int Cancel();
2 {
3   int_top(&CONF16);
4   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



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

```
00 61  ù²`¤.péËiü;....a
00 00  dvapi32.dll.....
32 2E  .....kernel32.
00 6D  dll.....m
00 00  svcrtdll.....
64 6C  .....user32.dl
00 77  l.....w
00 00  s2_32.dll.....
77 61  ...http=.\Softwa
69 6E  re\Microsoft\Win
72 73  dows\CurrentVers
65 74  ion\Internet Set
62 6C  tings.ProxyEnabl
43 4F  e.ProxyServer.CO
54 50  NNECT %s:%d HTTP
00 43  /1.0..... 200 .C
69 74  onsole.QuickEdit
00 00  .DbgPrint.....
00 00
```

Malware Profile: DBGPRINT



Government



Education



Think Tank



Finance



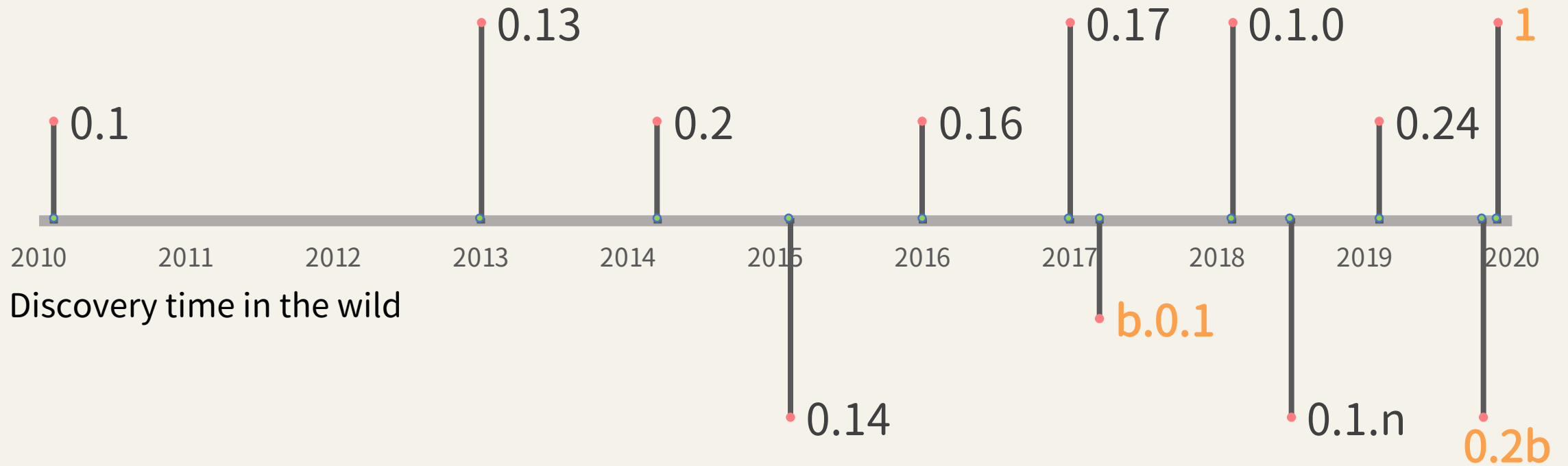
Technology



Healthcare

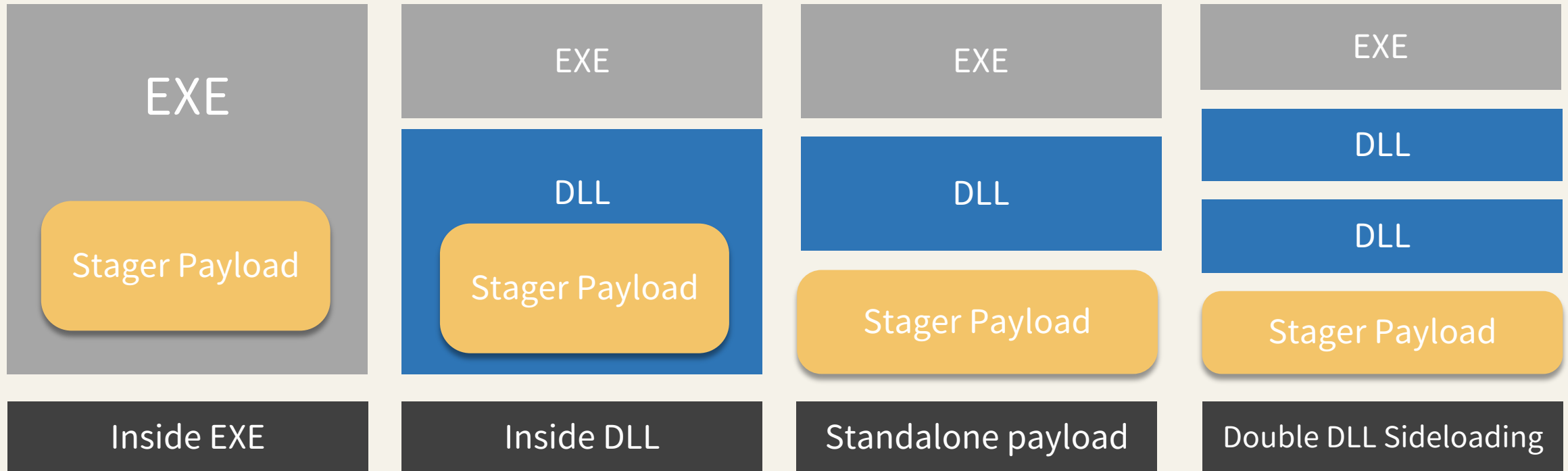
Evolution of DBGPRINT

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
```

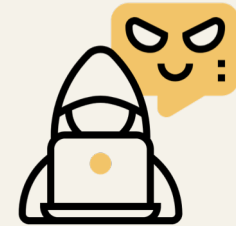
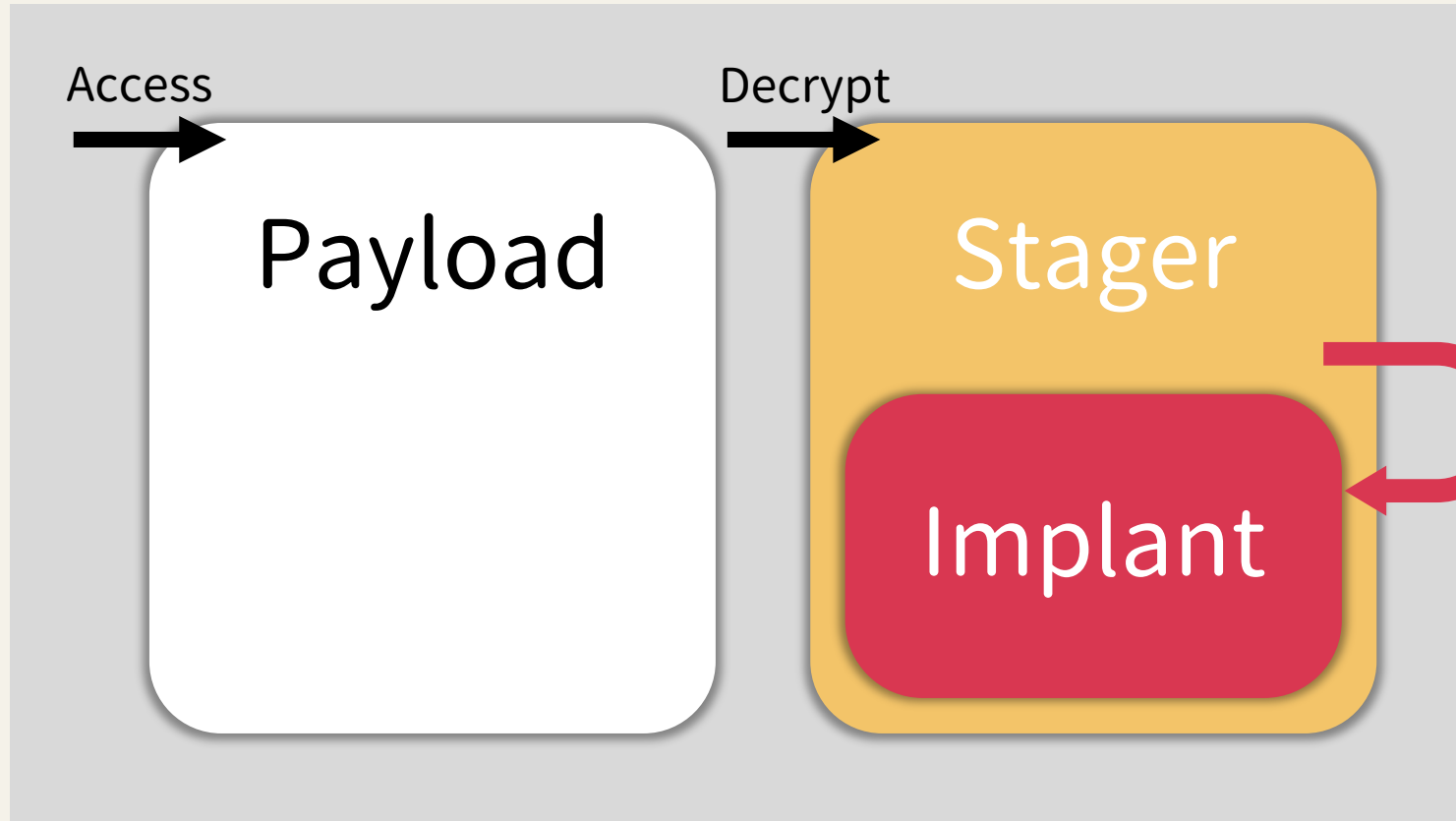
File path

Miss You! printupg.PNF

String + File name

In-Depth Analysis of DBGPRINT

Execution Procedure

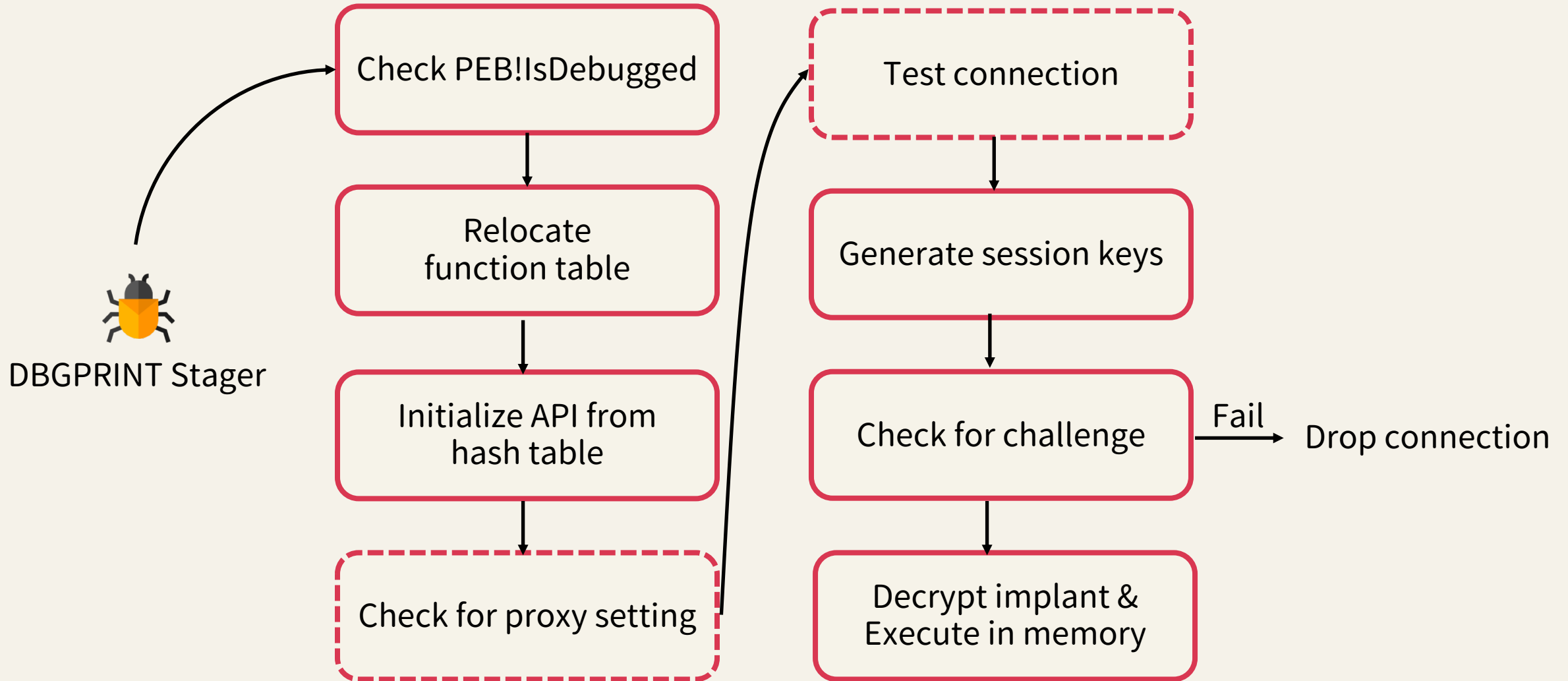


DBGPRINT Controller

- 1 Ask for DLL implant
- 2 Wait for connection

Inside DBGPRINT Stager

..... In some version



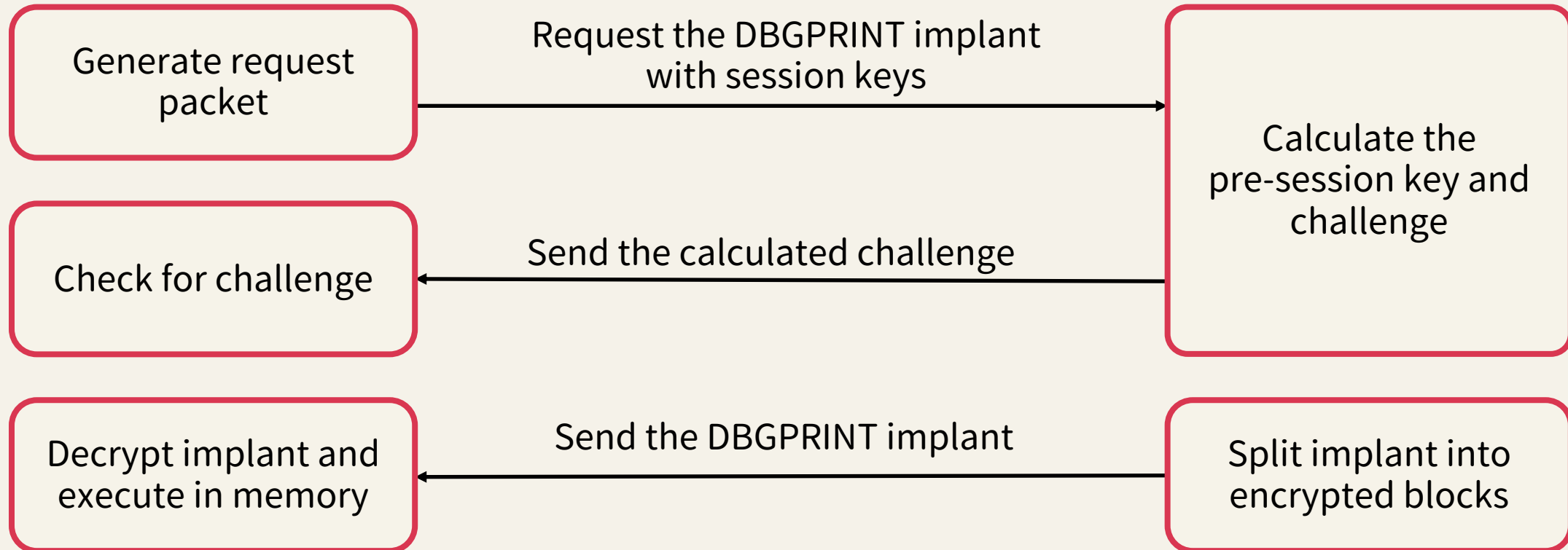
Inside DBGPRINT Stager



DBGPRINT Stager



DBGPRINT Controller



Inside DBGPRINT Stager

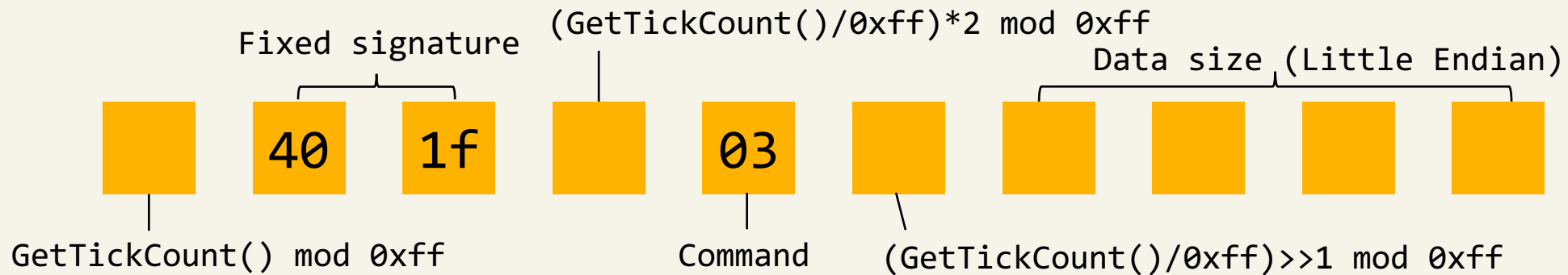


DBGPRINT Stager



DBGPRINT Controller

Generate request packet – Generate header



Inside DBGPRINT Stager



DBGPRINT Stager



DBGPRINT Controller

Generate request packet – Generate session keys

Authentication key \oplus Random number = Pre-session key

Pre-session key \oplus 0x6162636465666768696A6B6C6D6E6F00 = Session key 1

Pre-session key \oplus 0x01020304050607080900010203040506 = 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 \oplus 0x6162636465666768696A6B6C6D6E6F00 = Pre-session key

Pre-session key \oplus 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  $\oplus$  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

x64 Version

```
008F0049 rrrr  
008F004B 3D 40E80000 cmp     eax, 0E840  
008F0050 58          pop     eax  
008F0051 DB28       fld     tbyte ptr [eax]  
008F0053 C3         retn  
008F0054 64:A1 30000000 mov    eax, dword ptr fs:[30]  
008F005A 50          push   eax  
008F005B 5B          pop     ebx  
008F005C 8B03       mov    eax, dword ptr [ebx]  
008F005E 3D 00000100 cmp    eax, 10000  
008F0063 ^ 74 EB     ja     short 008F0050  
008F0065 v 75 01  
008F0067 E8 8D1DF7  
008F006C 40  
008F006D 0043 E2  
008F0070 v E3 6A  
008F0072 14 8B  
008F0074 C7
```

```
0000000000001D007C 3D 80E80000 cmp     eax,E880  
0000000000001D0081 58          pop     rax  
0000000000001D0082 DB28       fld     st(0),tword ptr ds:[rax]  
0000000000001D0084 C3         ret  
0000000000001D0085 6548:A1 6000000000000000 mov    rax,qword ptr qs:[60]  
0000000000001D0090 50          push   rax  
0000000000001D0091 41:5C      pop     r12  
0000000000001D0093 41:8B0424 mov    eax,dword ptr ds:[r12]  
0000000000001D0097 3D 00000100 cmp    eax,10000  
0000000000001D009C ^ 74 E3     je     1D0081  
0000000000001D009E v 75 01     jne   1D00A1  
0000000000001D00A0 E8 49C7C5A1 call  FFFFFFFFA1E2C7EE  
0000000000001D00A5 0000      add    byte ptr ds:[rax],al  
0000000000001D00A7 0049 FF   add    byte ptr ds:[rcx-1],cl  
0000000000001D00AA C5  
0000000000001D00AB E2 D8     loop  1D0085
```

Self-Modifying Code

```
H.\$.H.l$.H.t$ WATAUAVAWH..0.....XH..!.....H.....H.....QPH1.....XI.  
.u...I..C...M).L..PH..ATY.H1.....%h...X.(.eH.`.....PA\A..$=....  
t.u...I.....I....XYH..H...H...u...x...H..H.....E1.E1.H...N.....  
H..(...H.....E1.E1.H.....|.....E1.L.....L..h...1.H.....H.D$PH..  
vH.....(...I..H.....1.9+v3L.L$PL..(...A.M.L.....I..$H..tY..I  
...I...A.;+r...H.....r...q...H...H...p...H..H..I..H.....A..H..H.  
...P...H...h...H.\$XH.l$.H.t$hH..0A_A^A]A\_H.\$.WH.. 3.H..H..H;t<D.  
C.H.L$@.D$8..D$9..D$:..D$;.....D.8H..0D.?D.?0D..H...|.H.\$0H.._H  
.\$.UVWH..@D.....H.....H.....H.....H.....D.....H.....H.....  
.....u.H.....H.....H.....D.....H..8...H.....H..H...8...D..  
...H..8...H.....D.....H..@...H.....L.L$h`L.D$hH..H..  
..@...D.....H..@...H.....A...D.....H.....H.....D.D$h`H.T$  
hH.....D.....H.....H.....H.....H.....D.D$h`H.L$h3.....D.....  
H.. ...H.....A.....H..H.... ...D.....H.. ...H..H.....H..tv3.A..  
...H.....D.....H..0...H.....L...H.G.H.L$(H..L.\$ H.D$0H.|$8.....  
L.L$h`L..H..H...0...D.....H..0...H.....3.A.....H...8...H.L$h3.A..  
.....8...H.....H.....H.\$p.....H..@_`^].@SH.. H..H.....H..D..  
...H..p...H.....L..I..A..p...H.C.H.K.3.A.....8...L.[.H..A.....  
...H.. [.H.\$.H.l$.H.t$.WATAUH..p...D.....H..X...H.....H..3.....D  
.g.L..$P...A..H...X...D.....H..X...H.....D.G.H.T$0E3.H..78/..A..<1..M..F{.}.  
u.3..F...D.....H.....H.....H.T$h@H.....D.....H.....H.....  
|$D&r...l$DH.T$HE3.D.E.H.....t.D.....H..`...H.....U.L..$P..  
.H.L$E..`...D.....H..`...H.....A.MZ..fd9\$E..A.....Z{.}.H.L$ M.....  
.....k..+..@...@...H.T.@.....D.....H..X...H.....L..$`...H.L$h  
A...X...D.....H..X...H.....h...D.....H..P.....H..i.<.....H  
.T$h@A.....H...P...D.....H..P...H.....H.T$FH.L$0A.....M..D.d$h@D.l$
```

Before self-modifying

```
.....!.....P...ko....I_....GqI..@.U...#b7.;...-K(4q..).%.."..... .Z  
..O. C.U:<w....{.a.....N{.C...qgB.._z.....q....-N.a.b....s.7..&..s.#  
c0.31c.d.~.....[w"S.-.....V..`P...U..z....._#.VF.....U.`..&.A-/.}..  
....."90...U..O.a1miH.Yr0E.4.....Y.0=!...).!..08.Hd..Y.....mq.....  
j..v>...z.....gA0%...g@'.3..|'.|...&.....qk...qy1.q..8l...(77"l.  
.}.....d.X.7tF....]....,....1.....?4-.....}+G+'.....d.....  
...f}....t.q.D...N.....Y.a-.....q...6.....m.K..W.[{ygz.<).y.....  
8L...N4dx.....cc.....^..Z{.3."a.u.|D..eK.,....@.....p..  
.m.[.....kZ.|.<1.._W.Z{.}.kt.t.O.Y_.Z{.})....<1..I..Z{.}.qkt.t.y...  
C.zH...y...I...Z3.l....]3.jB...../."5.0.C.|...../."tt.y.Y.Z{.}).  
.kt.t.!(.....).....<13..s[[{H..V.u.<y=...Z3.m.F.u.<};.....?l.gZ.<)..  
!.....z..j<).q.C._...].ykt.....Z?.%..jt...B.....5..jt..u.#.|~  
..).l.<1..I3.Z{.}.kt.t.y.E/+..I./.....C.._..(..N...!.....j..j  
<)..C.._.....j5.41.C.|....].kt.x.1.....j<).y=.1`|[{H.<...p.C  
.....].ht.x.1.....j</...C..Y.o./h.".....]._h...ND..M.{1`|[{H  
...NT....._.....j0)...C.._KI./...].C.....H"/."i...A...7l...+..  
.1..Y..Z{.})...t.<1...C.yH.gZ6P..0.C..W.;..r.@SH.. H..H.....H..D..  
...H..p...H.....L..I..A..p...H.C.H.K.3.A.....8...L.[.H..A.....  
...H.. [.m.K.~~k.+[r#hp..0..^H..P.u.<y=...Z3..'jt.....1d|[{H.  
D.p...Y{H..Krv.<y=.v..Z3.1.B.u.<y;.....1..jt...A...../."i...B..T  
&_..]ge...u.....H.....<).%.....J=1..Ed.[{H.....=1.....l.-.  
j</p...].Z{.}.9kt.t.%#.....].ykt.}.....B..j..5]....F.\.....U.2c  
.4._.....,.....U.....n4]...C.._..I./....=1..E<+..I./....\2.C.z~[  
.)...<1..M..Z{.}.kt.t.}._Z{.1G.jt...VB...../.....P.....j<  
/h...v..Z{.})...$.<1..M..Z{.}.kt.t.}._Z{./{.,</p...s..Z{.})....|u>/.
```

After self-modifying

Only the wait-for-connection function is left

Double DLL Sideloading

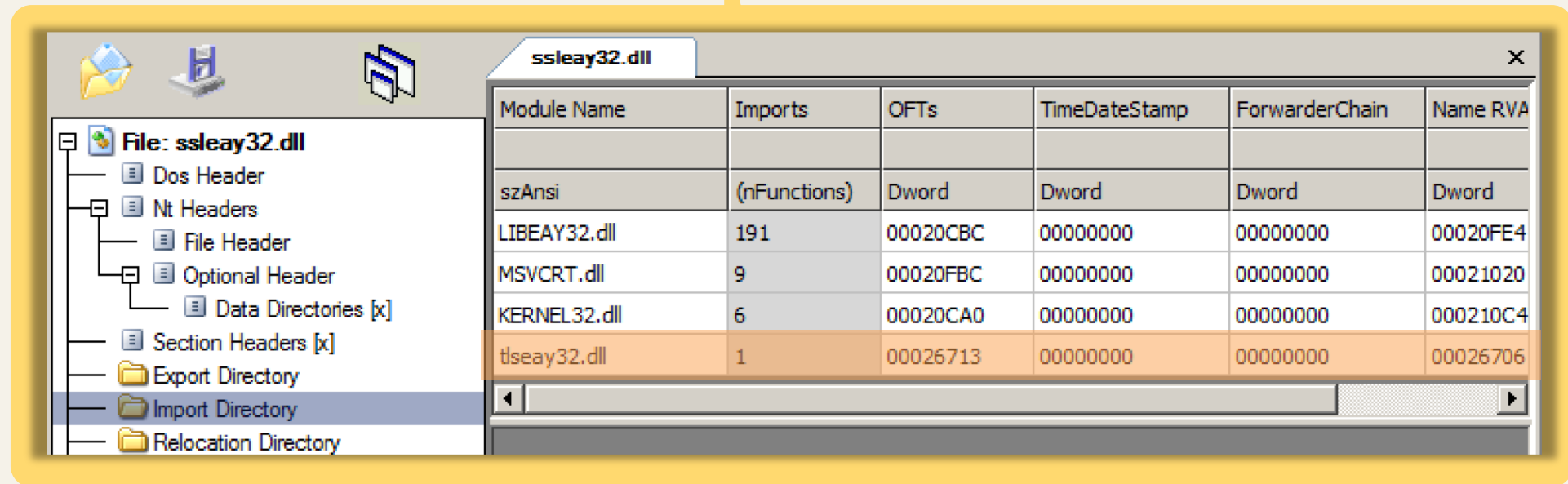
(White) Benign EXE



(Gray) Malicious DLL

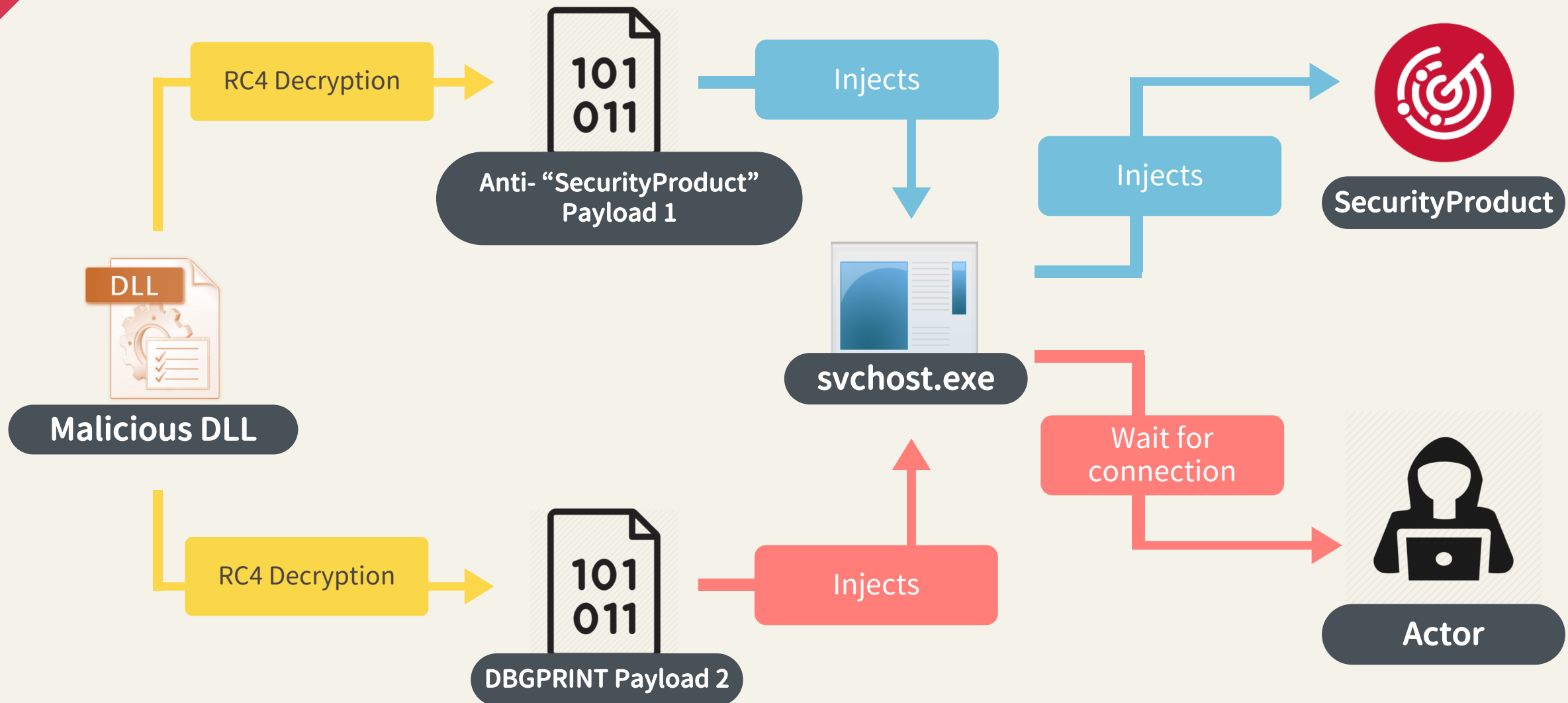


(Black) Malicious DLL



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword
LIBEAY32.dll	191	00020CBC	00000000	00000000	00020FE4
MSVCRT.dll	9	00020FBC	00000000	00000000	00021020
KERNEL32.dll	6	00020CA0	00000000	00000000	000210C4
tseay32.dll	1	00026713	00000000	00000000	00026706

Anti "SecurityProduct"



Questions?



TEAMT5
杜 浦 數 位 安 全

ycy@teamt5.org
aragorn@teamt5.org

