



TEAM T5

杜 浦 數 位 安 全

Japan Security Analyst Conference 2020

Evil Hidden in Shellcode:

DBGPRINTの進化

Malware Researcher

CiYi "YCY" Yu
Aragorn Tseng

Malware Researcher!



CiYi "YCY" Yu

1P

Malware Analysis
Campaign Tracking
Automated Analysis



Aragorn Tseng

2P

Malware analysis
Incident response
Machine learning

AGENDA



攻撃グループ「HUAPI」概要



マルウェア「DBGPRINT」概要



DBGPRINTの進化



DBGPRINTの仕組み



セキュリティ製品との鬼ごっこ



検出と対策



TEAM T5
杜 浦 数 位 安 全

攻撃グループ「HUAPI」概要



- ◆ 別名: BlackTech
- ◆ 活動: 2007~
- ◆ マルウェア:
 - ◆ TSCOOKIE
 - ◆ KIVARS
 - ◆ CAPGELD
 - ◆ DBGPRINT

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

BlackTech

Tweet Email

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

Even after we published the blog article in October 2018, we confirmed that the malware had not been updated.

Details of the fix

The malware copies its configuration to the memory. However, the configuration size is set to 0x1000 instead of 0x8D4.

```
1 signed int Cancel()  
2 {  
3     int i;   
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



マルウェア「DBGPRINT」概要

- ◆ 別名: Waterbear
- ◆ 2009 年以前から活動
- ◆ DLLエクスポート関数名“DbgPrint”
- ◆ 第二段階のマルウェア
- ◆ 高度なデザイン
 - ◆ Stager 経由方式を採用
 - ◆ プラグインシステム

00 61	ù²`¤.péËiü;....a
00 00	dvapi32.dll.....
32 2Ekernel32.
00 6D	dll.....m
00 00	svcrtdll.....
64 6Cuser32.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	

マルウェア「DBGPRINT」概要

標的となる業種



政府



教育



シンクタンク



金融



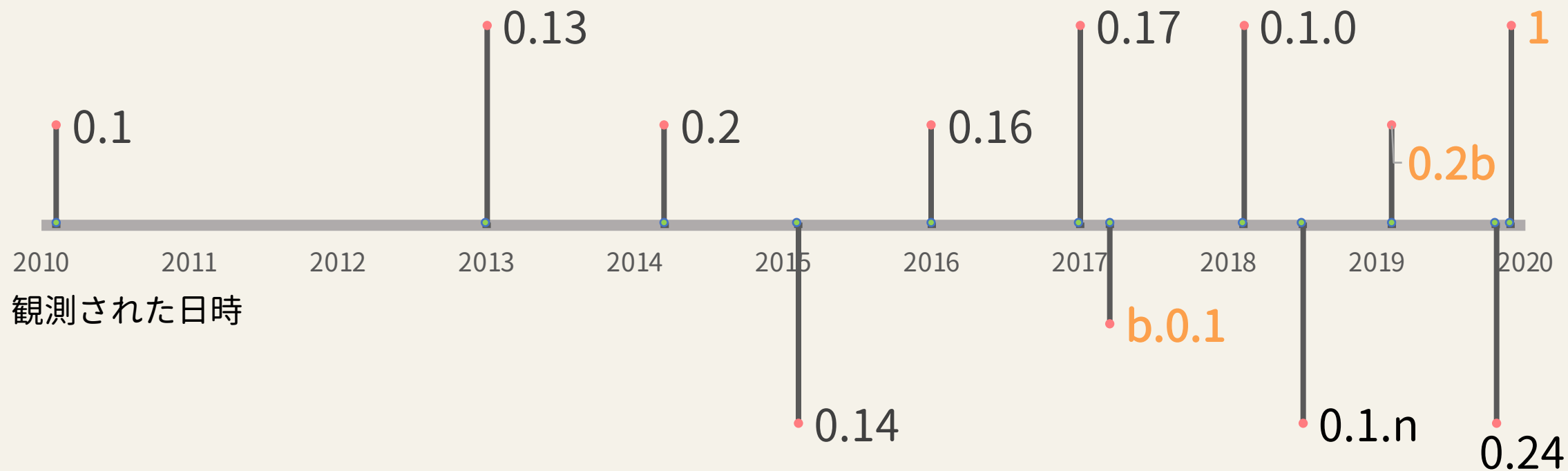
情報技術



医療

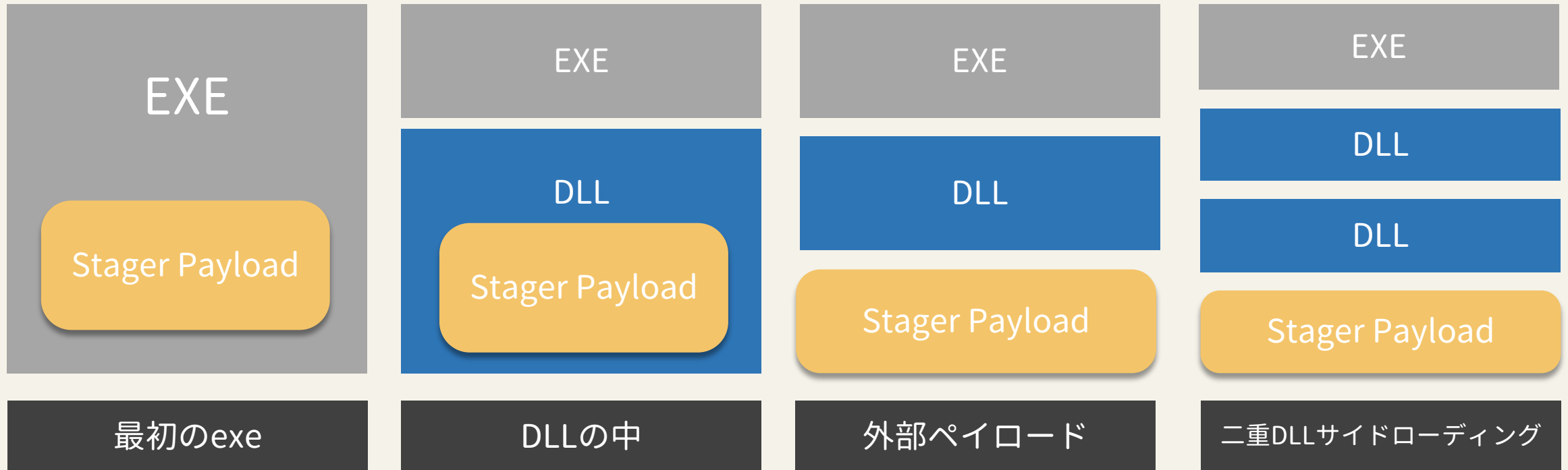
DBGPRINTの進化

バージョン観測



リッスンポート —

ペイロードの読み込み



ペイロードの RC4 キー

```
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 / ビットシフト

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

ランダムな16 Bytes

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

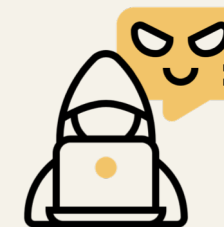
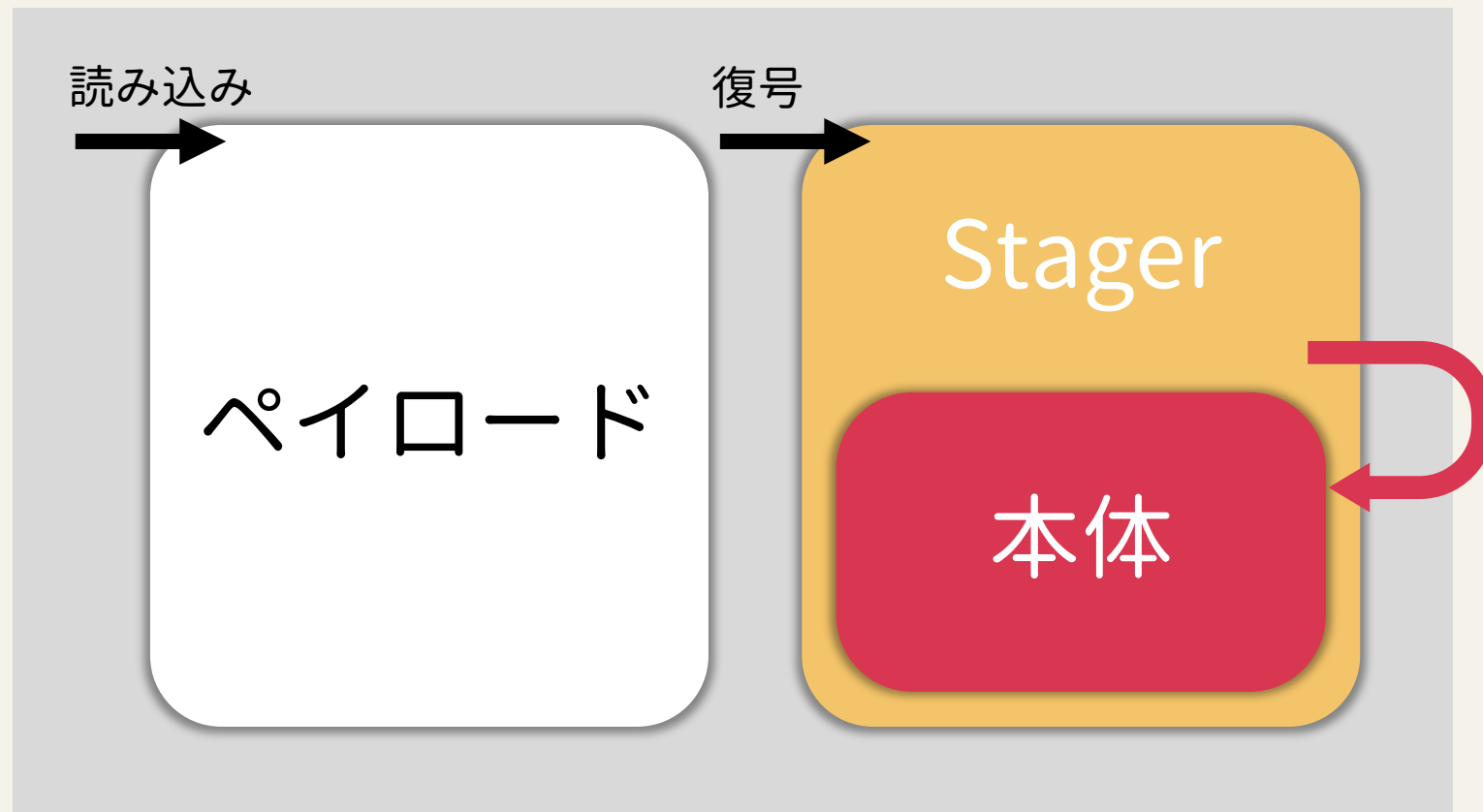
ファイルパス

Miss You! printupg.PNF

固定文字列 + ファイル名

DBGPRINTの仕組み

実行の流れ

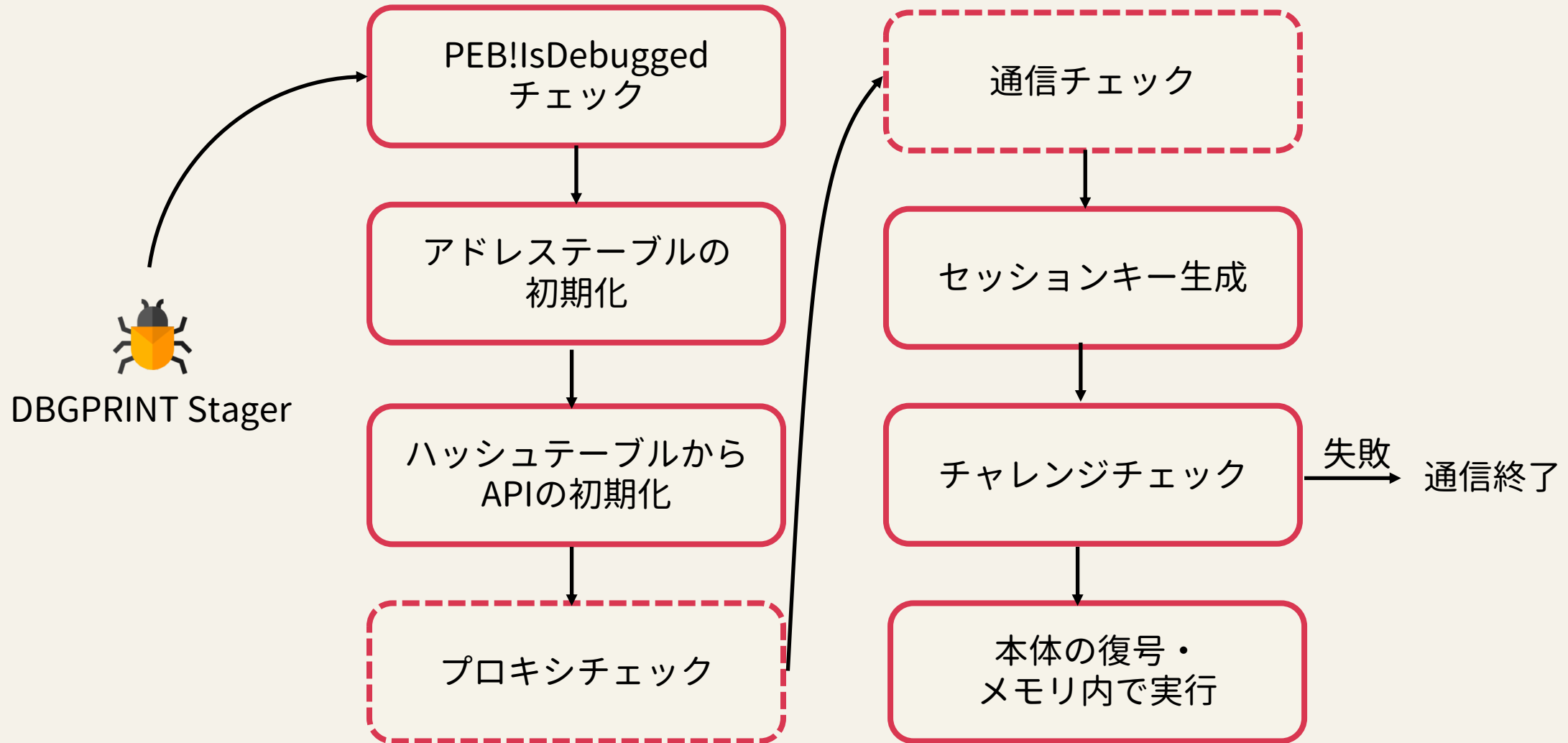


DBGPRINT コントローラ

- ① 本体を要求
- ② 通信を待つ

DBGPRINT Stagerの仕組み

..... 一部のバージョンのみ



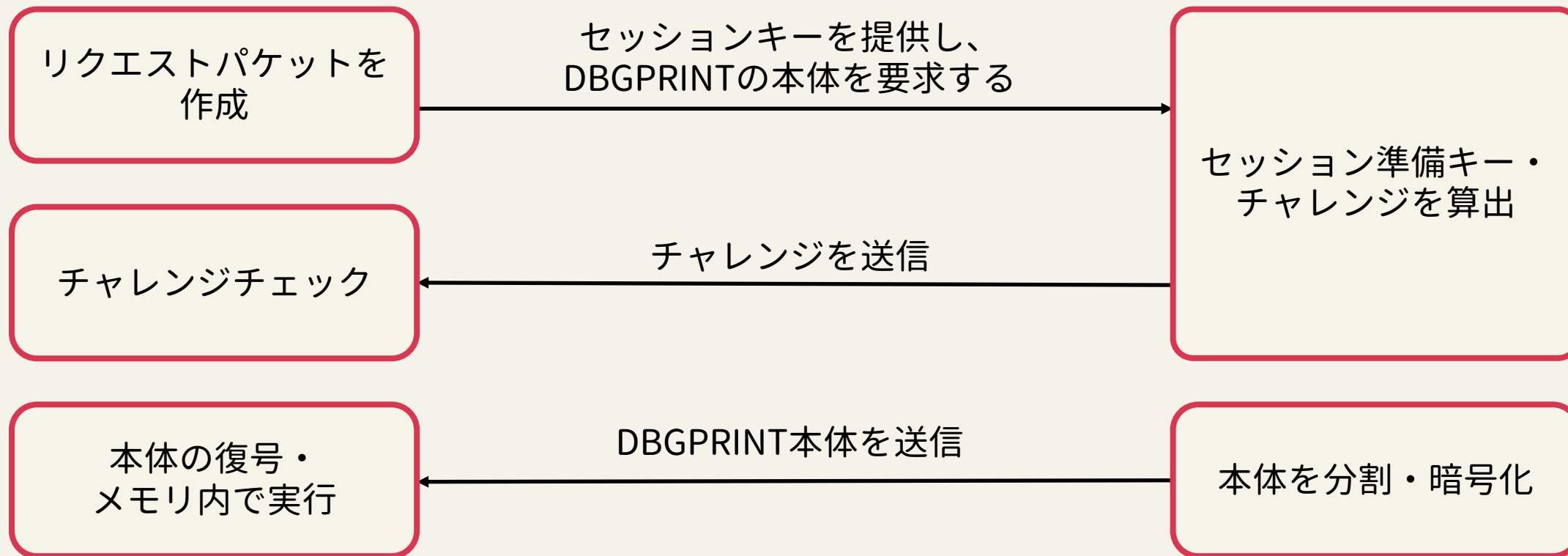
DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ



DBGPRINT Stagerの仕組み

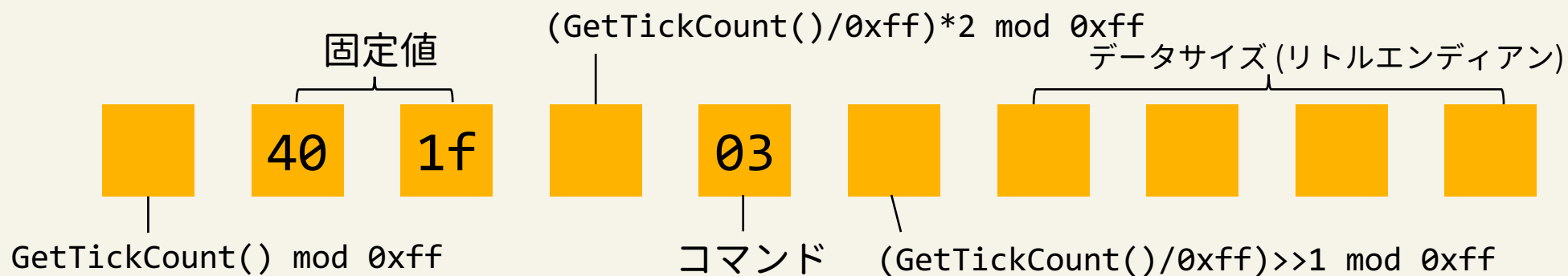


DBGPRINT Stager



DBGPRINTコントローラ

リクエストパケットの生成 - ヘッダ部分



DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

リクエストパケットの生成 - セッションキー

固定の認証キー \oplus 乱数 = セッション準備キー

セッション準備キー \oplus 0x6162636465666768696A6B6C6D6E6F00 = セッションキー 1

セッション準備キー \oplus 0x01020304050607080900010203040506 = セッションキー 2

DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

リクエストパケットの生成

本体をリクエストするコマンド

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	セッションキー 1
0000001A	55 a5 ba fc ce 02 64 97 3a 5c 43 77 dd 5d 47 43	セッションキー 2

DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

セッション準備キー・チャレンジの算出

セッションキー1 \oplus 0x6162636465666768696A6B6C6D6E6F00 = セッション準備キー
セッション準備キー \oplus 固定の認証キー = サーバからのチャレンジ

チャレンジコマンド

サーバからのチャレンジ

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	

DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

チャレンジチェック

if (サーバーからのチャレンジ ⊕ セッション準備キー) == 固定の認証キー:
- Yes: 続く
- No: 中止

DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

本体の暗号化と分割

```
# 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)
```

DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

本体の暗号化と分割

	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		
...			
...			

DBGPRINT Stagerの仕組み



DBGPRINT Stager



DBGPRINTコントローラ

本体の復号・メモリ内で実行

RC4_KSA(セッション準備キー)

復号ヘッダのサイズ = RC4_PRGA(PRGA_data1)

復号データのサイズ = Modified_RC4_PRGA(PRGA_data2)

復号ヘッダ = Modified_RC4_PRGA(PRGA_data3)

復号データ = Modified_RC4_PRGA(PRGA_data4)

DBGPRINT 本体

◆ ファイルの転送・管理

コマンドコード	機能
2	ドライブルIST
3	ファイルリスト
4	ファイルをC2にアップロード
5	ファイルをC2からダウンロード
6	ファイル名を変更
7	フォルダ作成
8	ファイルを削除
10	ファイルを実行
11	ファイルを移動
12	NtSetInformationFile

DBGPRINT 本体

◆ ウィンドウの管理・スクリーンショット

コマンドコード	機能
807	ウィンドウリスト
808	ウィンドウを非表示
809	ウィンドウを表示
810	ウィンドウを閉じる
811	ウィンドウを最小化
812	ウィンドウを最大化
814	スクリーンショット
815	スクリーンショットオブジェクトに対しSetEvent()する

DBGPRINT 本体

- ◆ リモートデスクトップ
- ◆ プロセス/ネット通信/ サービス管理

コマンドコード	機能
816	リモートデスクトップ
817	プロセスリスト
818	プロセスを終了
820	ネット通信状態
821	ネット通信を中断
822	サービスリスト
827	サービス操作

DBGPRINT 本体

◆ リモートシェル・レジストリ管理

コマンドコード	機能
1006	リモートシェルを開始
1007	リモートシェルを終了
1008	リモートシェルのPIDを取得
2011	レジストリリスト
2013	レジストリキーの作成
2014	レジストリキーを変更
2015	レジストリキーを削除
2016	レジストリキーの値を削除

セキュリティ製品との鬼ごっこ

パターンの抹消

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

Mutex

[illegible]

M

}8ºýáÈÒßŒî3ù.¿R-
 ,...ø.24.....

îïñíîñîîêñîî
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyyyy
 yyyyyyyyyyyyy©a..

q.ßä®;©ò

スペース (0x20)

パターンの抹消

```
1213141516.....  
è...0.1.....  
...Mutex.....  
....usr.narllab.  
com.....  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .»P.
```

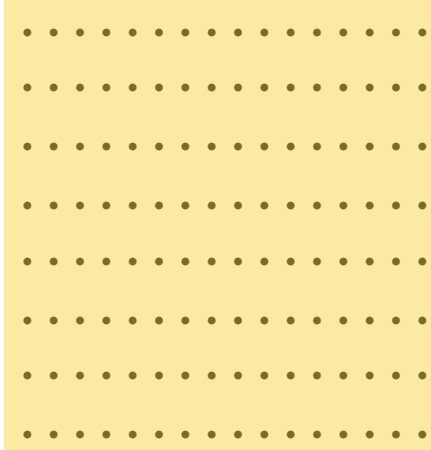
```
. . . . .  
abcdefghijklmno.  
./e.Oó{-cÓF5Ç².ä
```

オリジナル

[illegible]

XOR with 0xff

```
F.P...M...~...H1  
....b.0.1.....  
....M.....
```



```
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....
```

```
.....  
.....abcdefgh  
ijklmno../e.0.{-
```

リッスンポート

x64 版

```
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 008F0065
008F0065 v 75 01     jne    short 008F0067
008F0067 E8 8D1DF7 40          fld     st(0), tword ptr ds:[rax]
008F006C 40          fld     st(0), tword ptr ds:[rax]
008F006D 0043 E2     ret
008F0070 v E3 6A     je     1D0081
008F0072 14 8B     jne    1D00A1
008F0074 C7         call   FFFFFFFFA1E2C7EE
                add byte ptr ds:[rax], al
                add byte ptr ds:[rcx-1], cl
                ???
                loop 1D0085
```

```
0000000000001D007C
0000000000001D0081
0000000000001D0082
0000000000001D0084
0000000000001D0085
0000000000001D0090
0000000000001D0091
0000000000001D0093
0000000000001D0097
0000000000001D009C
0000000000001D009E
0000000000001D00A0
0000000000001D00A5
0000000000001D00A7
0000000000001D00AA
0000000000001D00AB
```

```
3D 80E80000
58
DB28
C3
6548:A1 6000000000000000
50
41:5C
41:8B0424
3D 00000100
^ 74 E3
v 75 01
E8 49C7C5A1
0000
0049 FF
C5
E2 D8
```

```
cmp     eax, E880
pop     rax
fld     st(0), tword ptr ds:[rax]
ret
mov     rax, qword ptr qs:[60]
push    rax
pop     r12
mov     eax, dword ptr ds:[r12]
cmp     eax, 10000
je      1D0081
jne     1D00A1
call    FFFFFFFFA1E2C7EE
add     byte ptr ds:[rax], al
add     byte ptr ds:[rcx-1], cl
loop    1D0085
```

自己書き換え

```
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.|$8.....
L.L$L 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$@E3.H.....
u.3..F...D.....H.....H.....H.T$@H.....D.....H.....H.....
|$D&r...l$DH.T$HE3.D.E.H.....t.D.....H..`...H.....U.L..$P..
.H.L$E..`...D.....H..`...H.....A.MZ..fD9\$E..A.....H.L$ M.....
.....k..+..@...@...H.T.@.....D.....H..X...H.....L..$`...H.L$
A...X...D.....H..X...H.....h...D.....H..P.....H..i.<.....H
.T$@A.....H...P...D.....H..P...H.....H.T$FH.L$0A.....M..D..d$@D.l$
```

実行前

```
....!....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.
..z8/...A.....)....<1..M..Z{.)..kt.t.}..]_Z{./h."...q.p.._...Z-.j.Z.
D.p...Y{H..Rnv.<y=V..Z3.i.B.u.<y;.....1..jt...A...../."i...B..T
&_..]ge...u.....H.....<).%.....J=1..Ed.[{H.....=1.....1.-.
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>/.
```

自己書き換え後、
残されたのはポートをリッスンするコードのみ

二重DLLサイドローディング

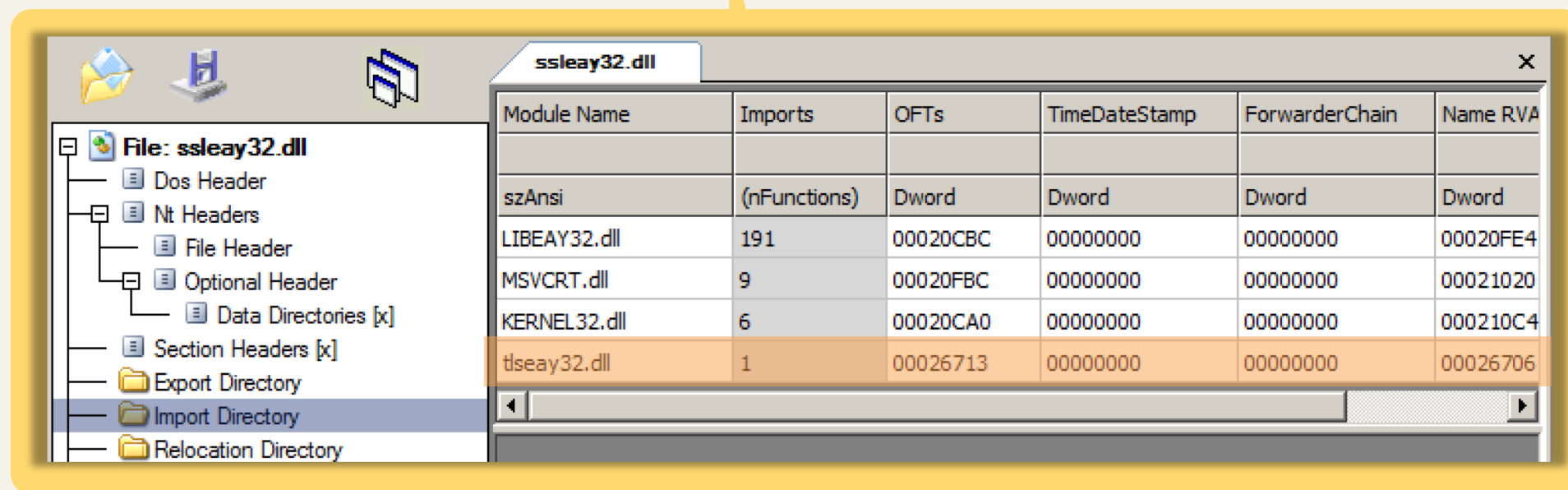
正常なEXE (ホワイト)



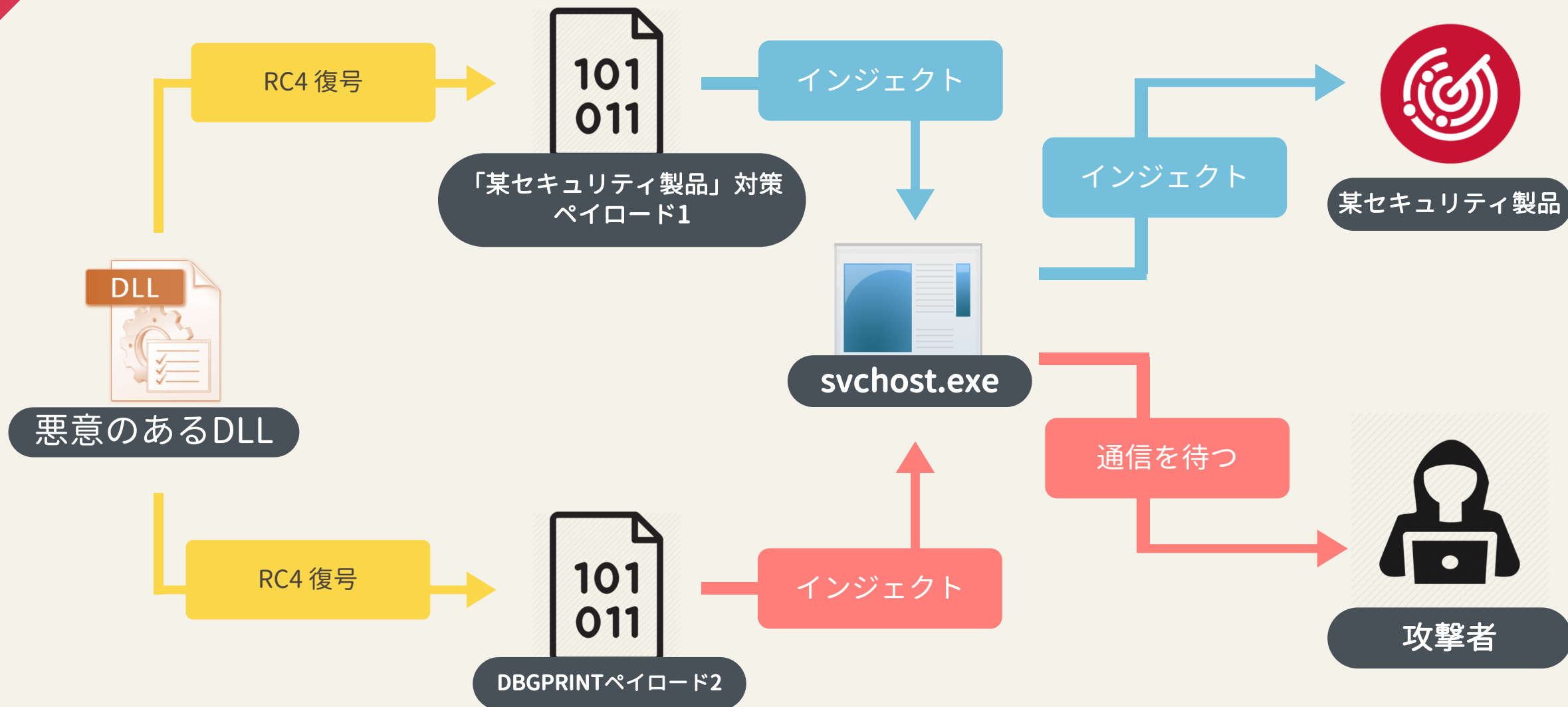
悪意のあるDLL (グレイ)



悪意のあるDLL (ブラック)



「某セキュリティ製品」対策



質疑応答



TEAM T5
杜 浦 數 位 安 全

ycy@teamt5.org
aragorn@teamt5.org

