TEAMT5
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!

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

- 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

TEAMT5
杜浦數位安全

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 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

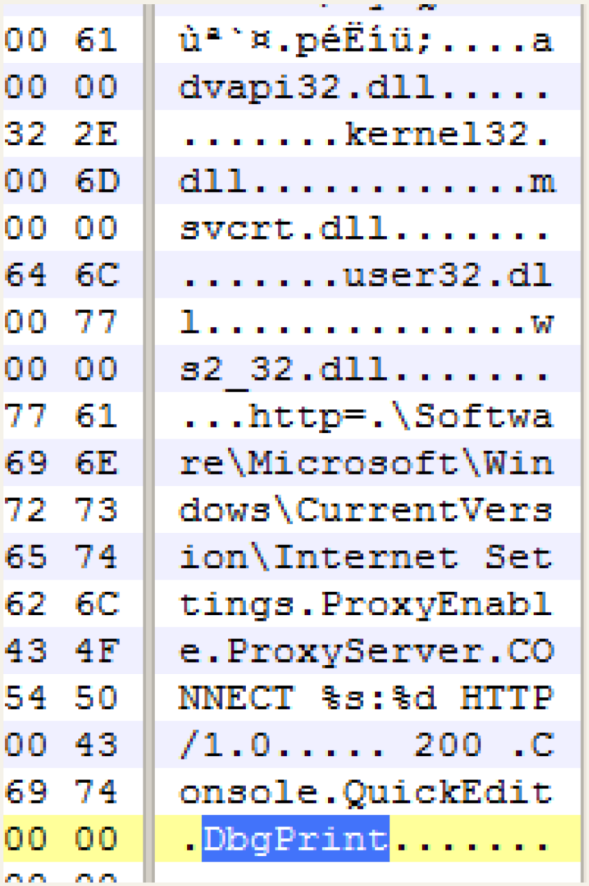
Figure 1 describes the flow of TSCookie’s execution.

Figure 1: Overview of TSCookie

TSCookie EXE

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



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

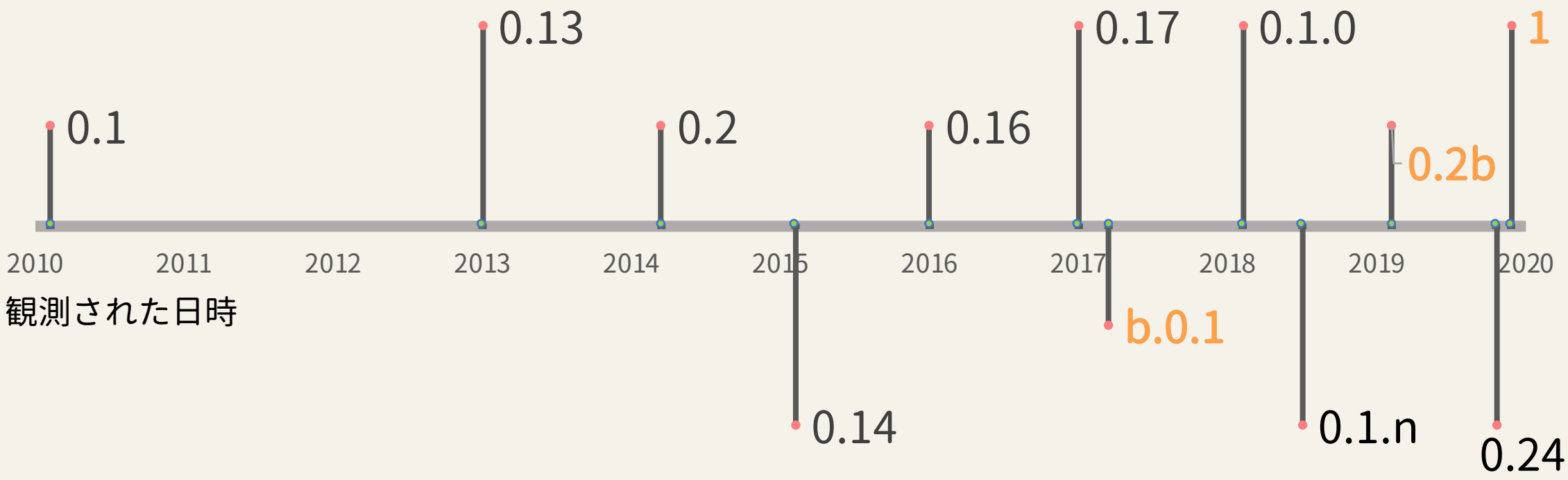
金融

情報技術

医療

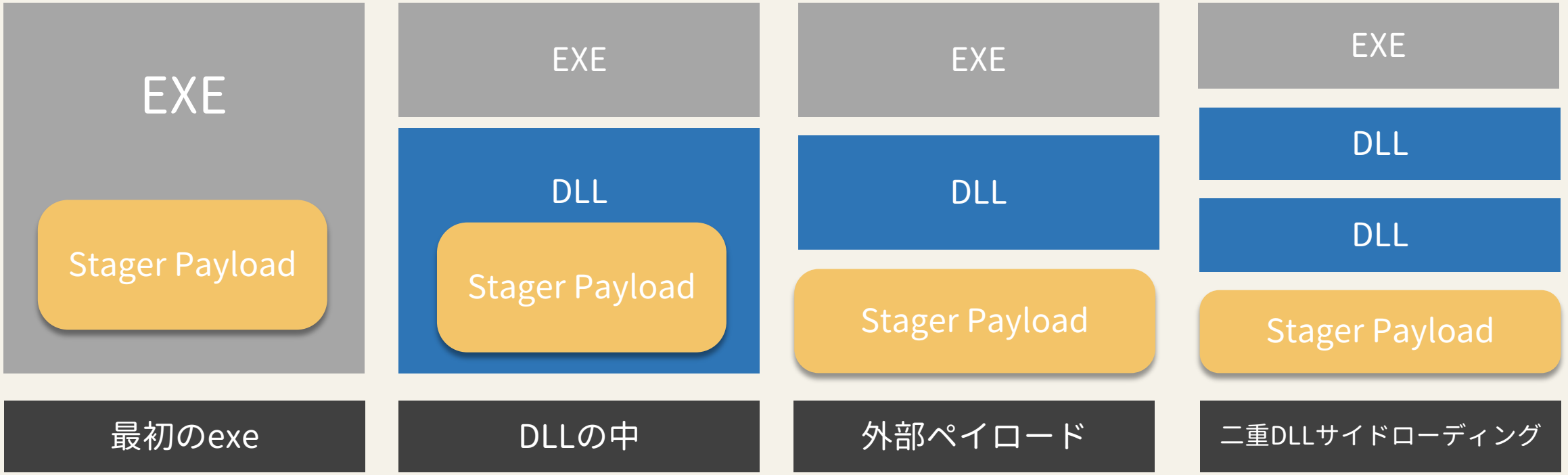
DBGPRINTの進化

バージョン観測



リッスンポート

ペイロードの読み込み


EXE
Stager Payload
EXE
DLL
Stager Payload
EXE
DLL
Stager Payload
EXE
DLL
DLL
Stager Payload
最初のexe
DLLの中
外部ペイロード
二重DLLサイドローディング

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

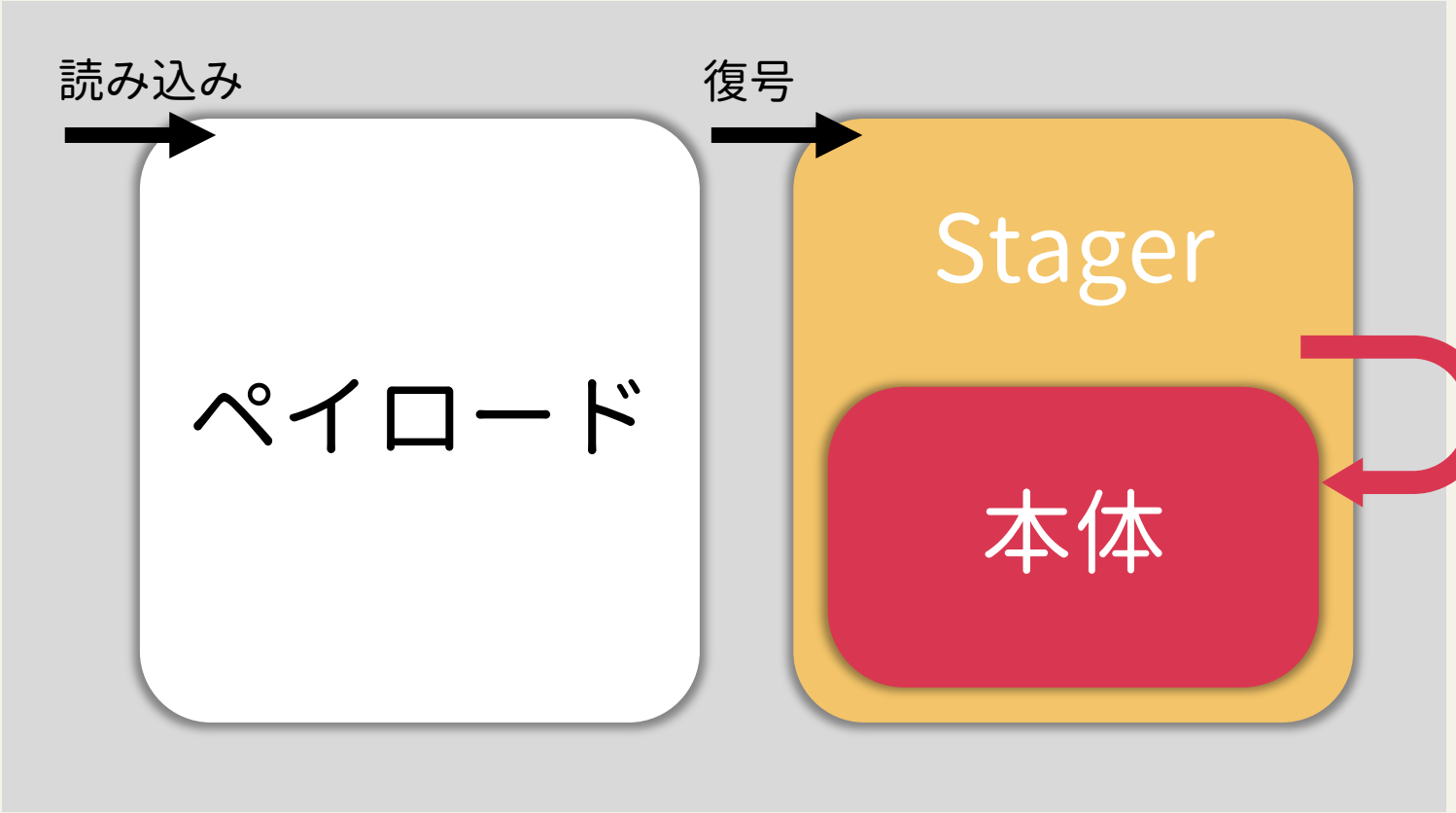
ファイルパス

Miss You! printupg.PNF

固定文字列 + ファイル名

DBGPRINTの仕組み

実行の流れ



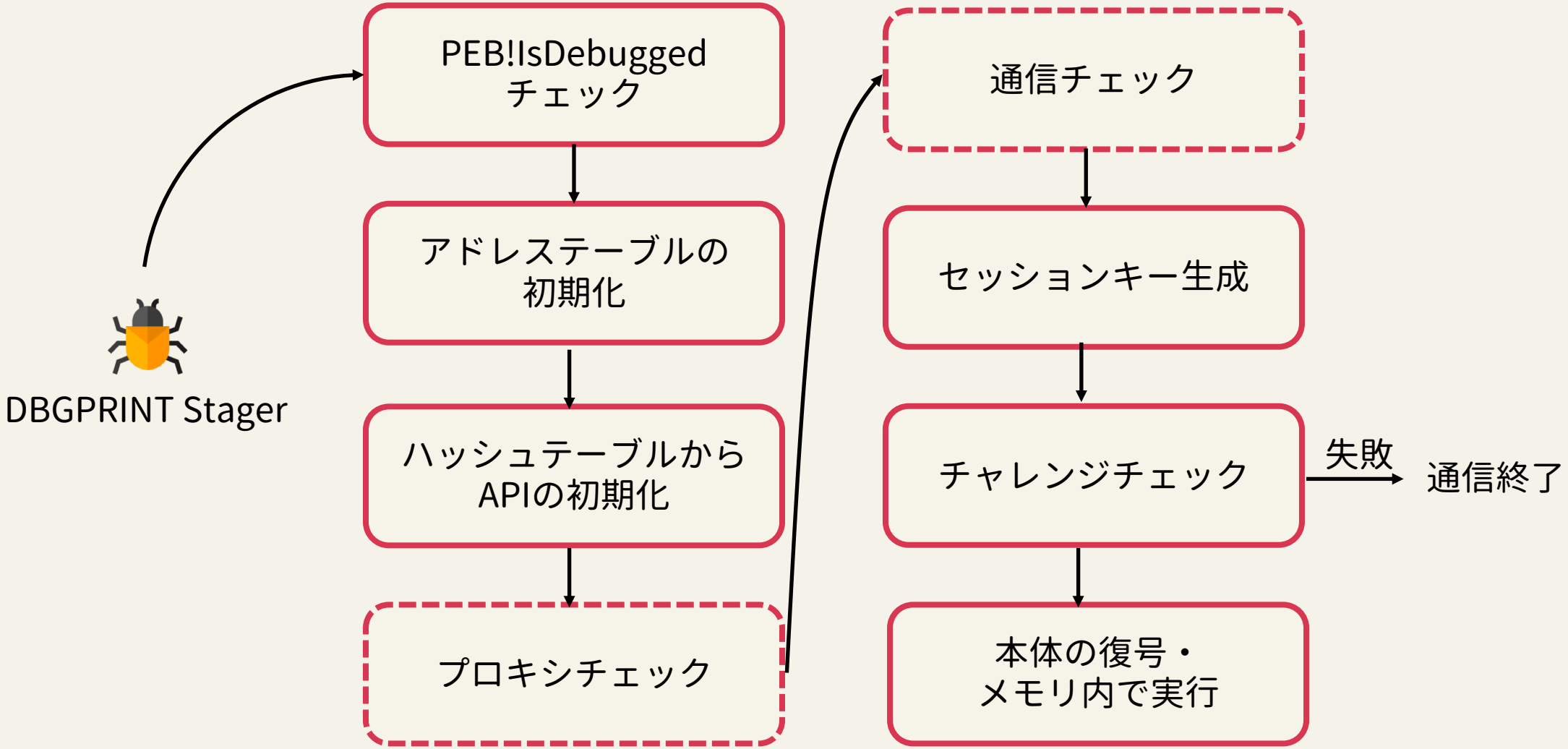
DBGPRINT コントローラ

❶ 本体を要求

❷ 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

リクエストパケットを作成

セッションキーを提供し、DBGPRINTの本体を要求する

セッション準備キー・チャレンジを算出

チャレンジチェック

チャレンジを送信

本体の復号・メモリ内で実行

DBGPRINT本体を送信

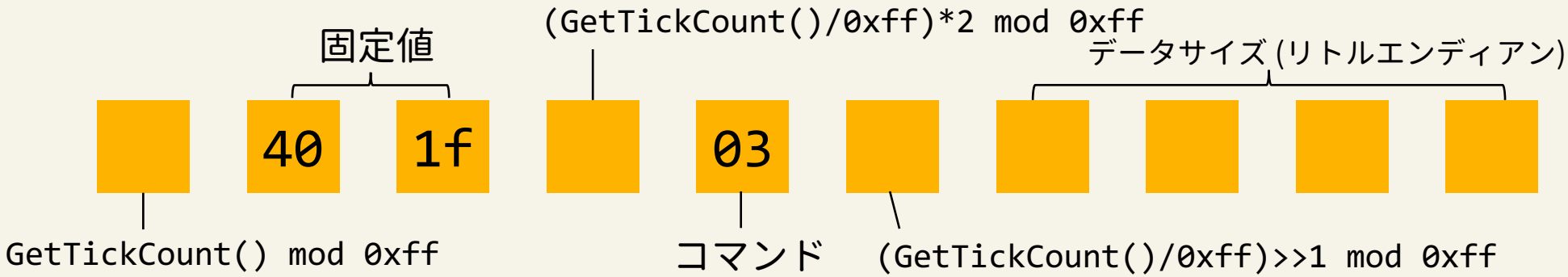
本体を分割・暗号化

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 ⊕ 乱数 = セッション準備キー

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

セッション準備キー ⊕ 0x0102030405060708090001020304050 6 = 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 ⊕ 0x6162636465666768696A6B6C6D6E6F00 = セッション準備キー

セッション準備キー ⊕ 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	ドライブリスト
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

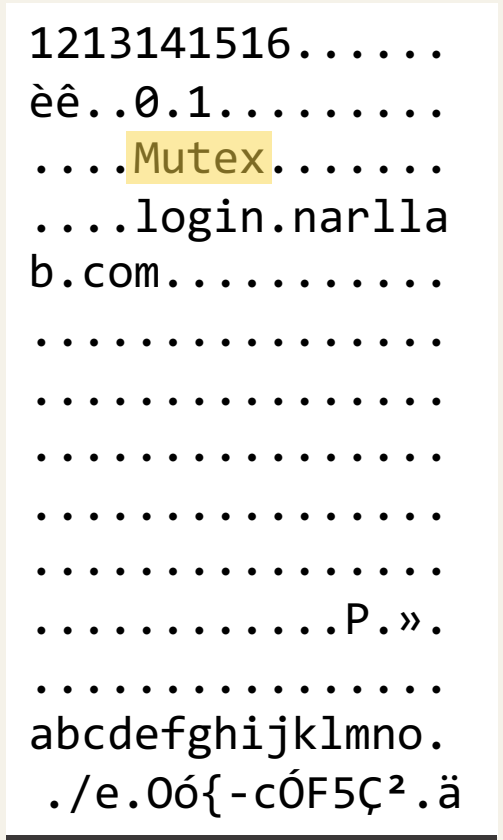
DBGPRINT 本体

- リモートシェル・レジストリ管理

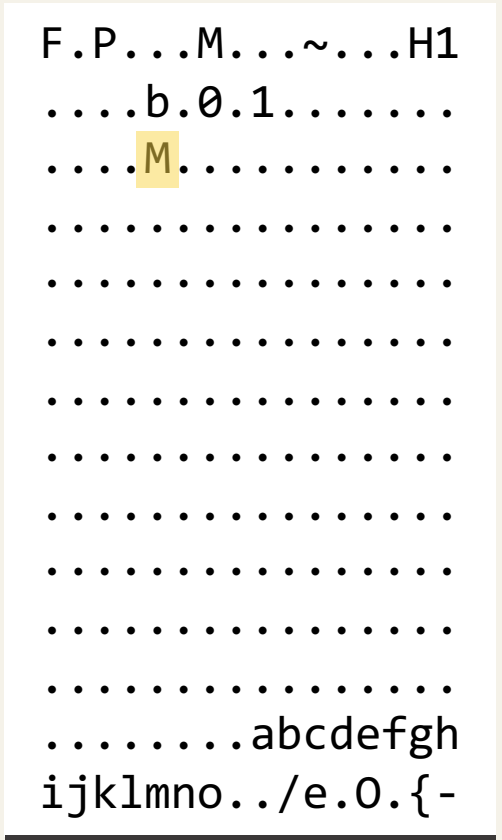
コマンドコード	機能
1006	リモートシェルを開始
1007	リモートシェルを終了
1008	リモートシェルのPIDを取得
2011	レジストリリスト
2013	レジストリキーの作成
2014	レジストリキーを変更
2015	レジストリキーを削除
2016	レジストリキーの値を削除

セキュリティ製品との鬼ごっこ

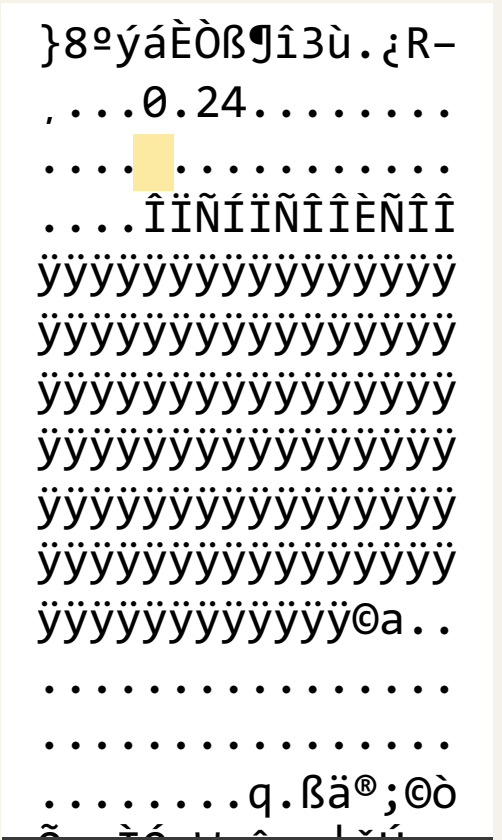
パターンの抹消



Mutex

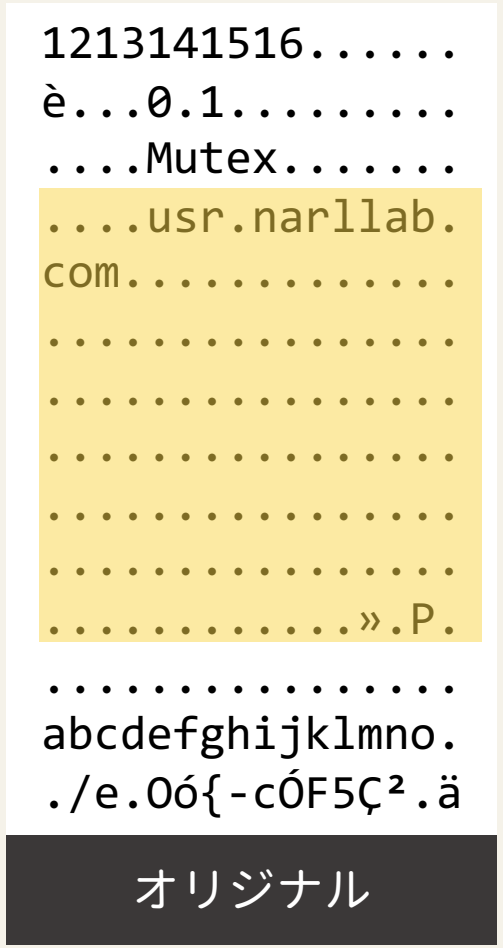


M

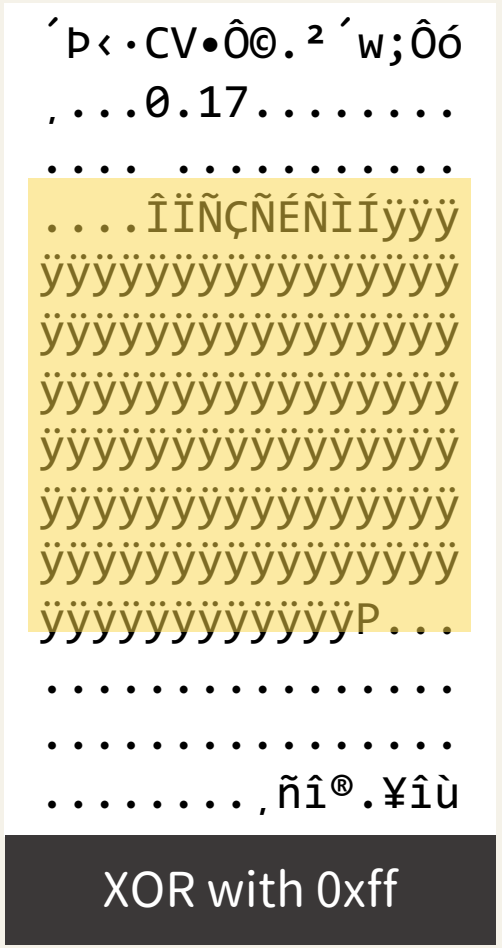


スペース (0x20)

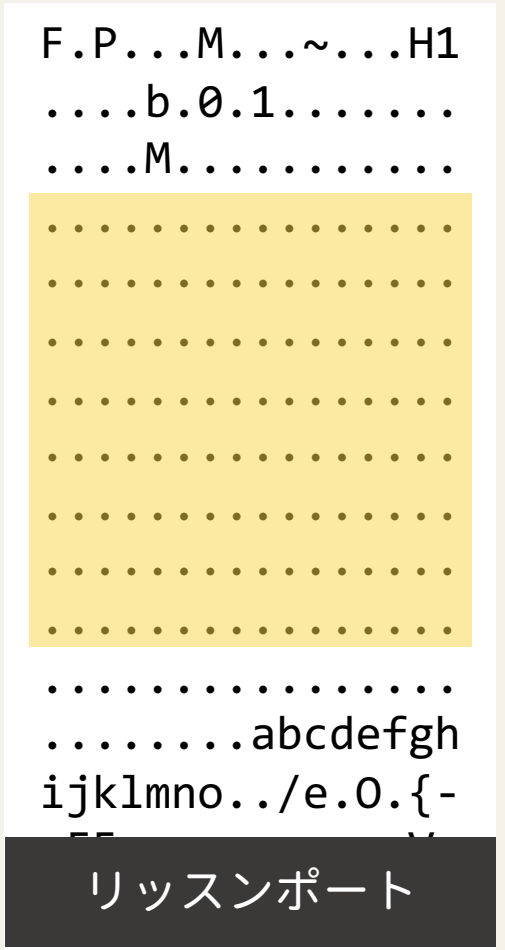
パターンの抹消



オリジナル

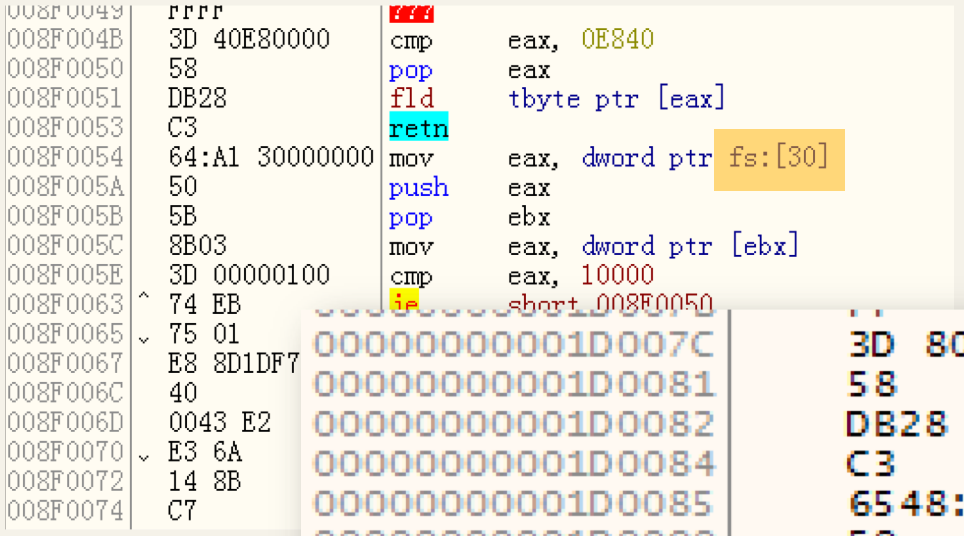


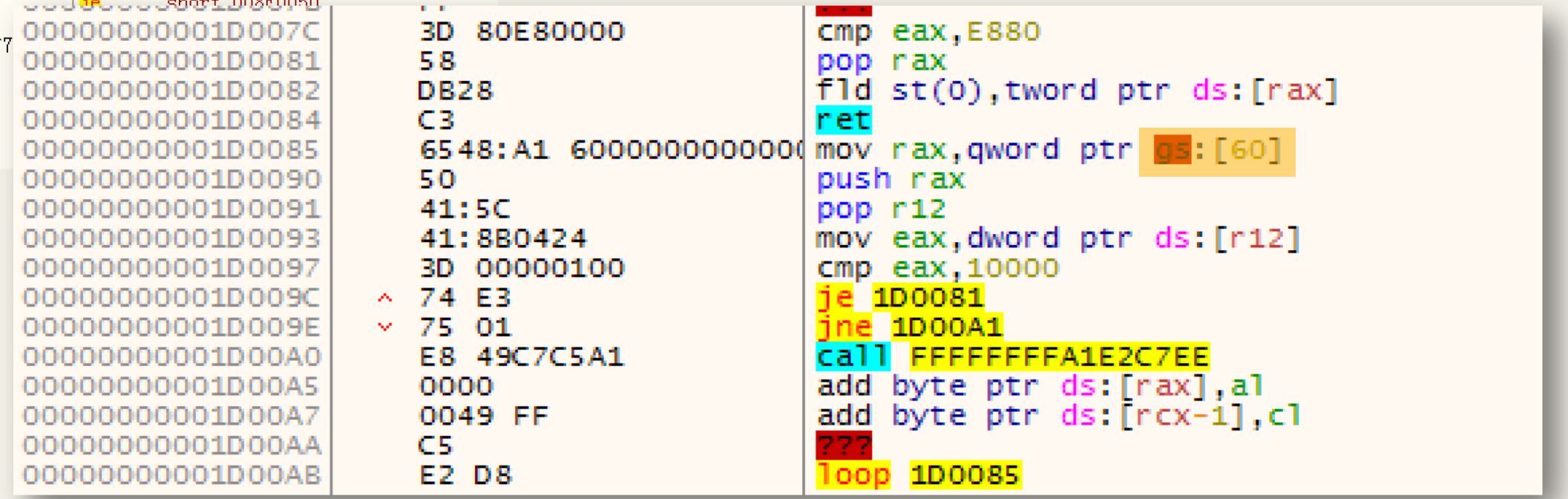
XOR with 0xff



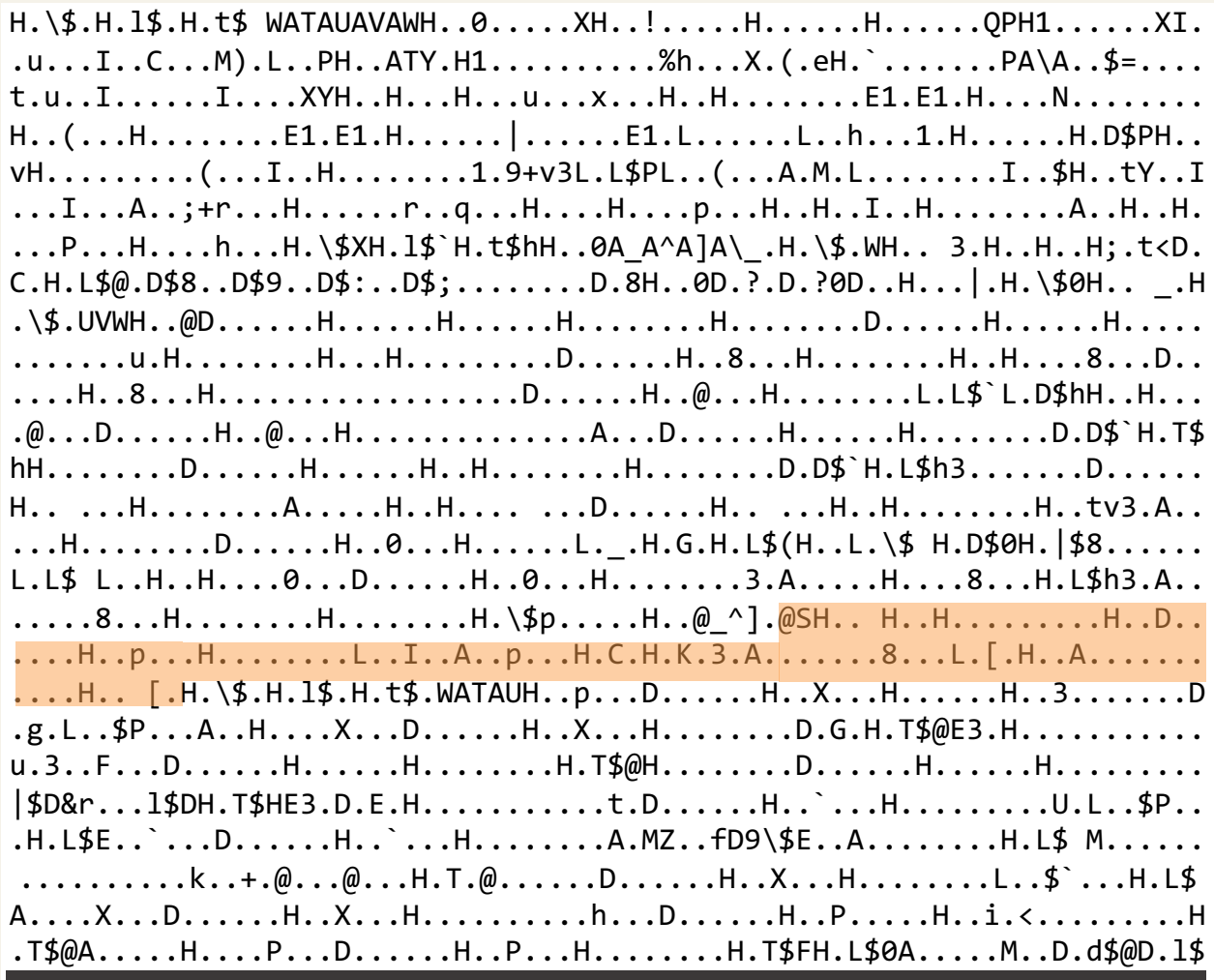
リッスンポート

x64 版

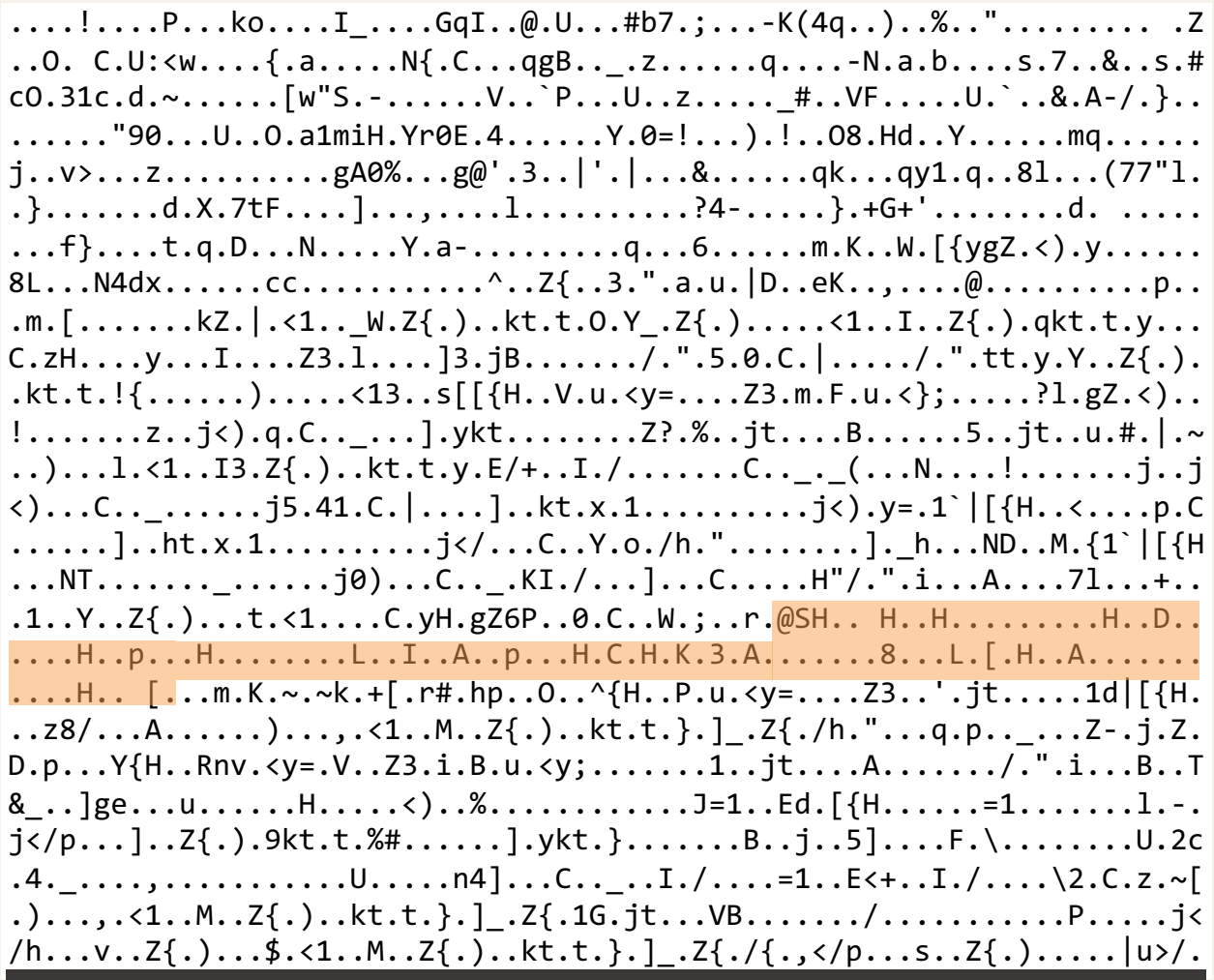




自己書き換え



実行前



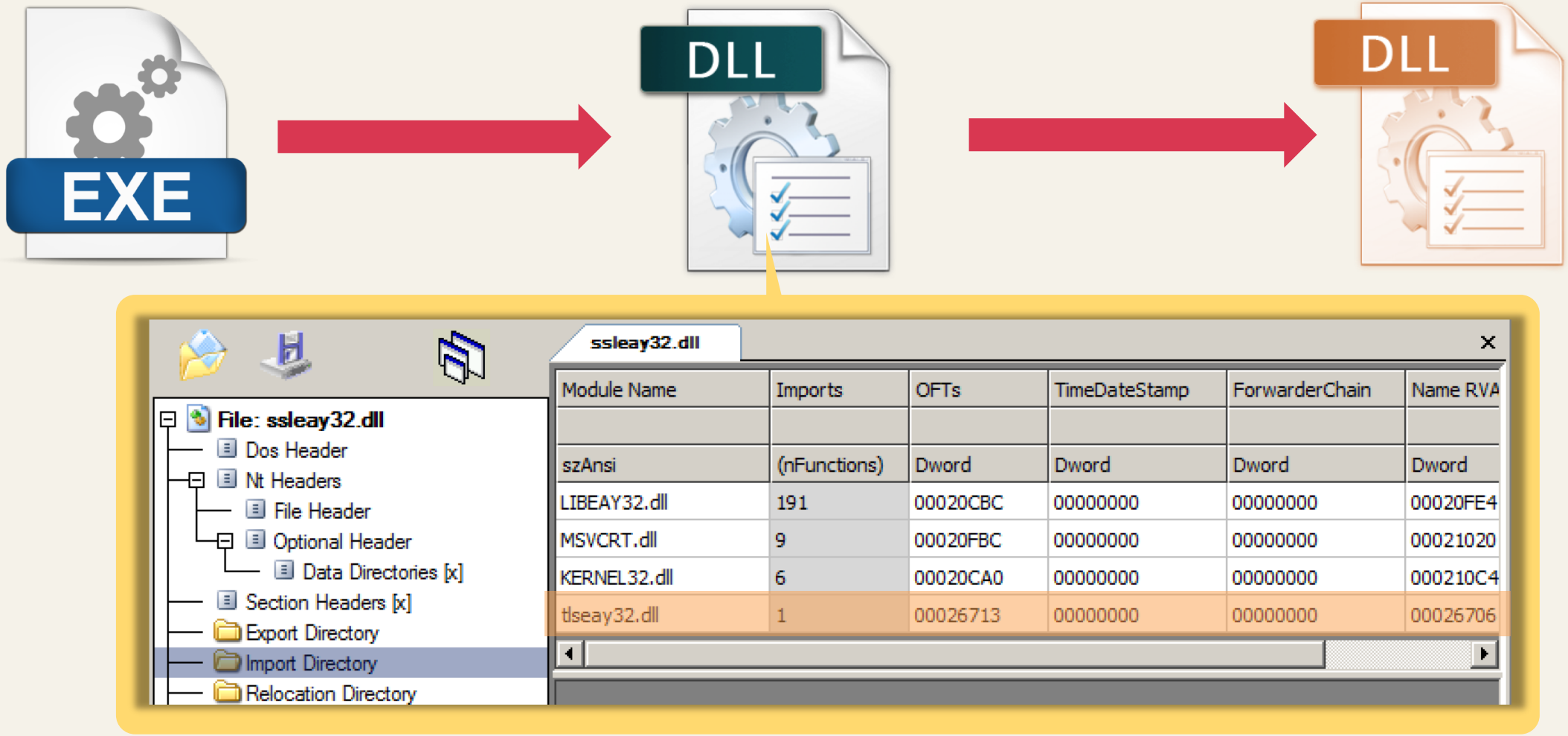
自己書き換え後、
残されたのはポートをリッスンするコードのみ

二重DLLサイドローディング

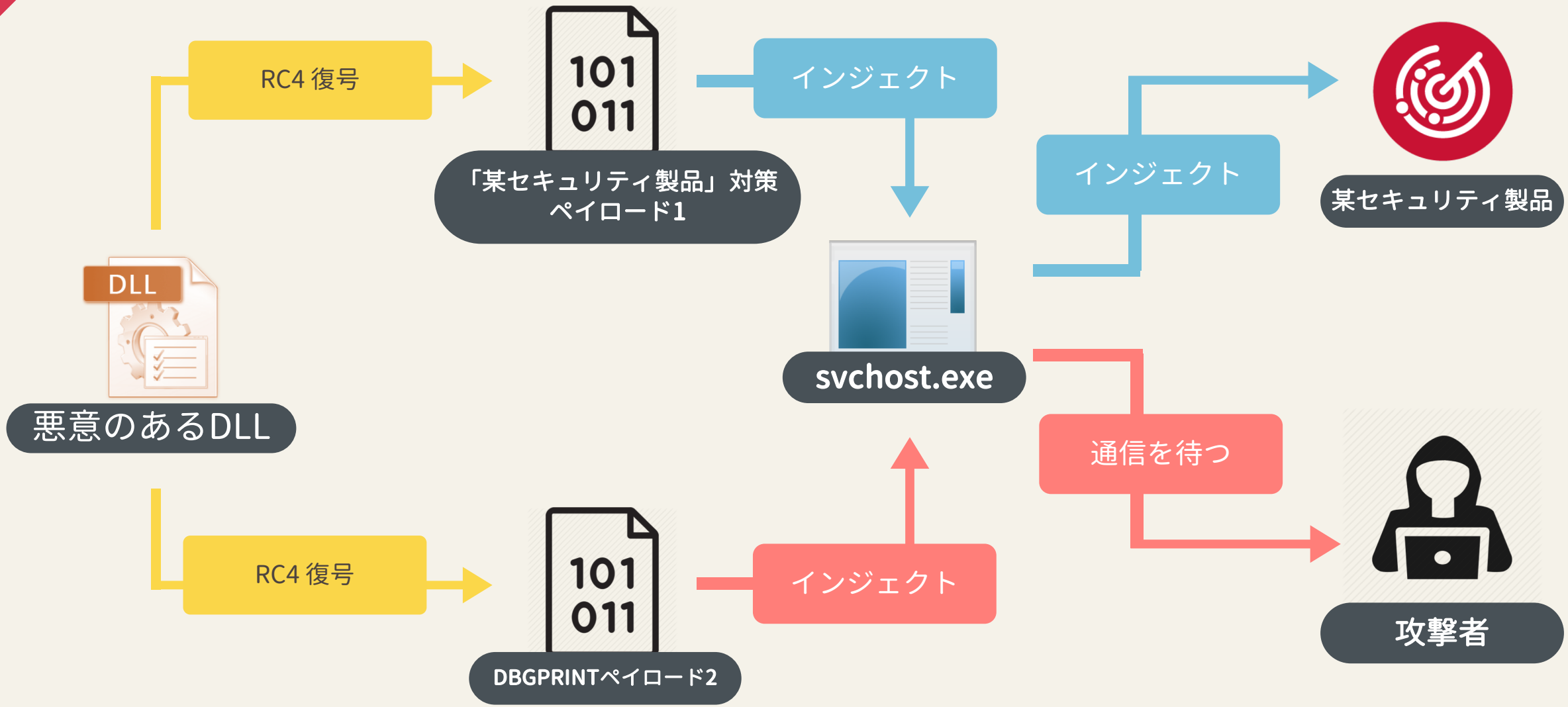
正常なEXE (ホワイト)

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

TEAMT5
杜 浦 數 位 安 全

ycy@teamt5.org
aragorn@teamt5.org