Himawariの異常な暗号

または私は如何にして心配するのを止めて暗号を解読するようになったか

中津留 勇

SecureWorks Japan 株式会社

Counter Threat Unit

2018/01/25
Japan Security Analyst Conference 2018

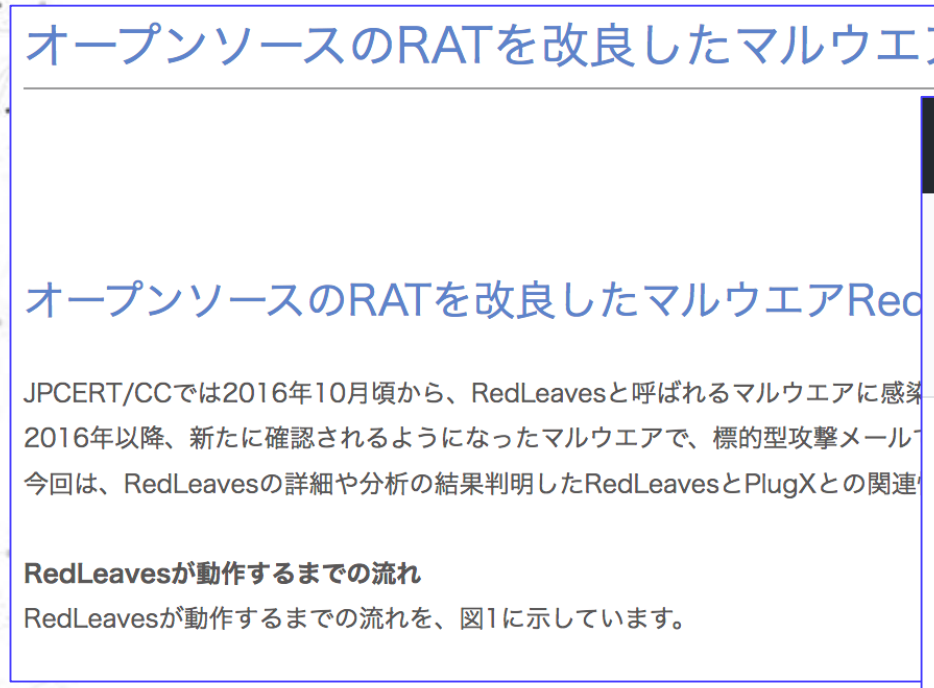
背景

RedLeaves

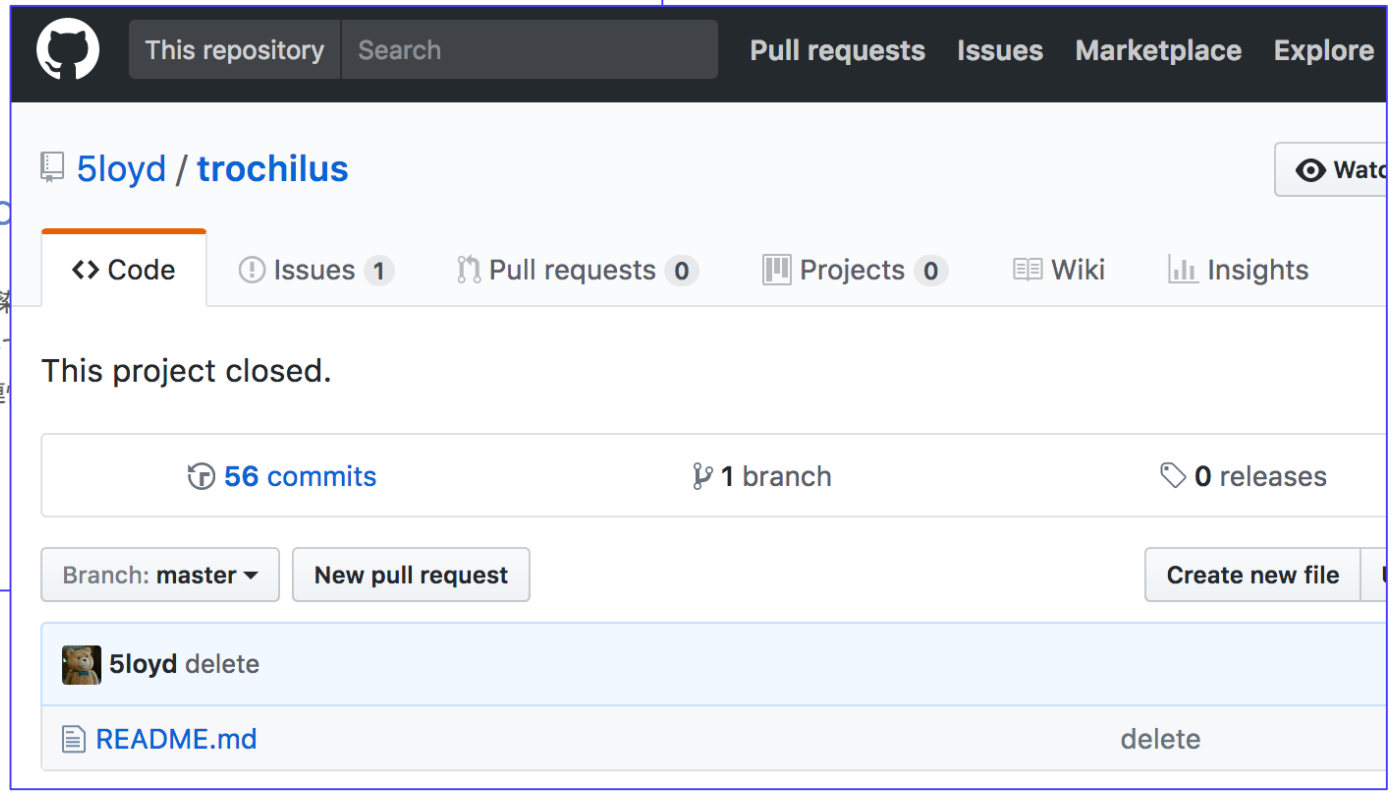
標的型攻撃で使用される RAT

- 2016年10月頃から日本における複数の標的型攻撃で確認

オープンソースのRATを改良したマルウエアRedLeaves(2017-04-03)



https://www.jpcert.or.jp/magazine/acreport-redleaves.html



https://github.com/5loyd/trochilus

Himawari

RedLeaves の亜種

- 2017年4月頃から確認（2017年9月頃からよく見かける印象）
  - 暗号方式の変更など
  - Office 文書のマクロ or 埋め込みオブジェクトで感染

- 「RedLeaves（レッドリーブス）」
  RedLeaves は、ファイルを利用しないオープンソースの RAT である「Trochilus（トロチラス）」のような挙動を示すバックドア型マルウェアで、第二ステージで利用されます。Trochilus は、感染 PC 上で情報を探索することが知られています。また、RedLeaves には PlugX の機能が採用されています。2017 年 4 月には、「himawari（ヒマワリ）」と名付けられた RedLeaves の亜種が確認されています。この亜種は、当時リリースされた YARA ルールによる検出を回避する能力を備えていました。

■ChessMaster と menuPass は同一のサイバー諜報活動集団

サイバー諜報活動集団「menuPass」は、関心を持つ標的が利用する MSP を狙って標的型攻撃キャンペーン「Operation Cloud Hopper（クラウドホッパー作戦）」を実行した集団です。その悪名は、標的型メールから感染および攻撃に至る執拗な活動と共に、さまざまな情報窃取型マルウェアと脆弱性攻

http://blog.trendmicro.co.jp/archives/15551

Himawari

Virus Total で取得可能な検体情報（インストーラのみ）

登録日時 (JST)	SHA-256 ハッシュ値	ファイル名
2017-09-05 07:17:02	a16ae1e5b919dfbc211d071af94278fee3aa8b62c6ff63126cb3f648ed4feeec	関係資料.doc.scr
2017-09-09 14:33:57	68edcbfcf985688bea2e9780e5aa3a90723ae0ab3a1e82f85d873e8a262daf62	TestDrawer.exe
2017-09-13 13:45:44	bb7398405e1b09ec53191c919dbebf5a9bf308a64832e299e57adf6f878c4f8e	講演会お知らせ（29年10月）doc.exe
2017-09-21 11:29:54	72f0e6a6f41301fcf02fe9e0bf5640210bd1a28dad6024e5eab97af8e87290e3	平成29年度　秋の艦船電波会ゴルフコンペ.doc.exe 関係資料.doc.exe

マルウェアの暗号処理の実装不備？

Emdivi の例

t19 と t20中期

- MD5文字列に add 演算および sscanf するため鍵空間が小さくなる
  - 総当たりによる鍵特定が可能

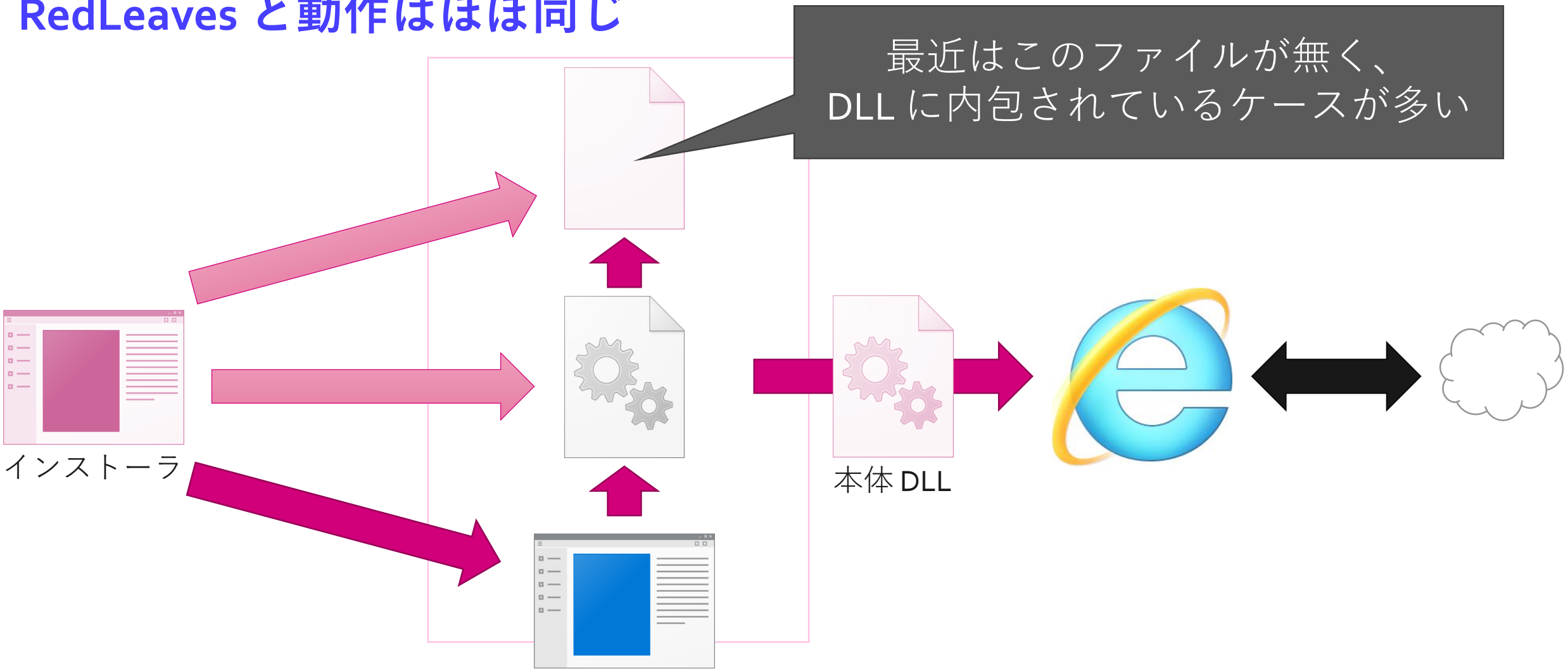
t20.30.4242.2091.4209.0

- 2017年6月にサブミットされた検体
  - 6a104646464f3bb53857869 4acf29ce3ae430892073d85d001b3891c1456c86a
- MD5 を16進数表記にする際のオフセット指定ミスがあり検体内の文字列を正しく復号できないバグが存在
  - advapi32 の MD5 API を使用しようとした際のミス？

Himawari の暗号処理解析

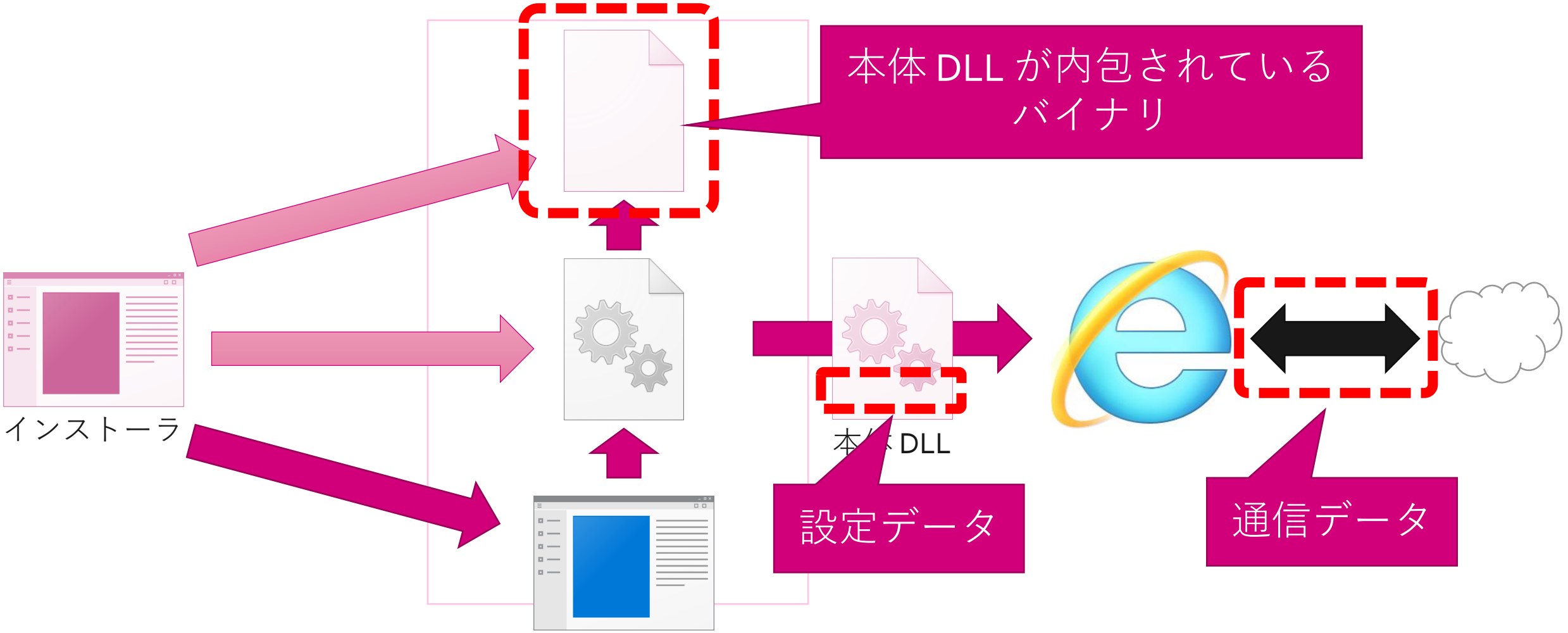
Himawari の動作

RedLeaves と動作はほぼ同じ



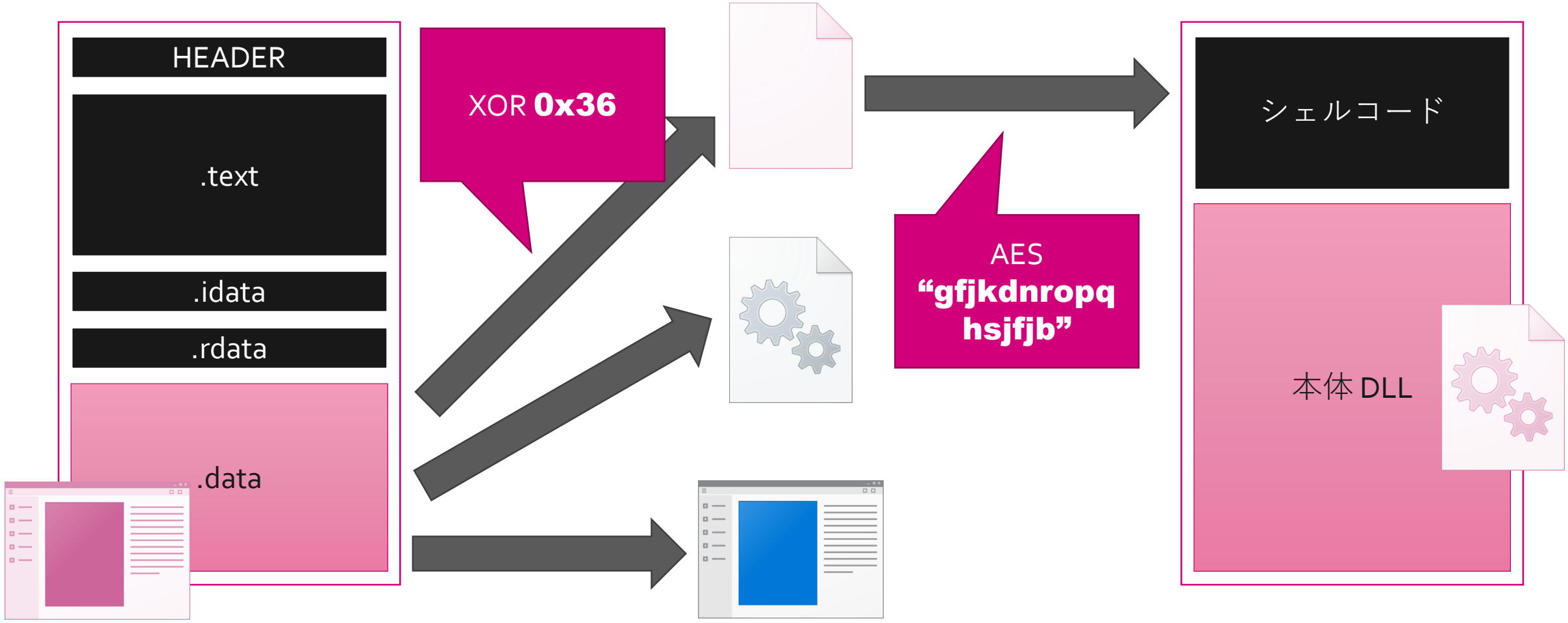
Himawari が暗号化しているデータ

ファイルと通信データをそれぞれ暗号化



ファイルの暗号化（一例）

XOR だけだったり、暗号鍵が変更されたり、いくつかのパターンが存在



異常な DES

設定と通信データの処理で使用されている

暗号化されたデータが 8バイト単位で繰り返す

- ECB モード？

FindCrypt では DES の定数がヒットする

```
0x73ABE3D8: found const array DES_ip (used in DES)
0x73ABE418: found const array DES_fp (used in DES)
0x73ABE458: found const array DES_ei (used in DES)
0x73ABE488: found const array DES_p32i (used in DES)
0x73ABE4E8: found const array DES_sbox2 (used in DES)
0x73ABE528: found const array DES_sbox3 (used in DES)
0x73ABE568: found const array DES_sbox4 (used in DES)
0x73ABE5A8: found const array DES_sbox5 (used in DES)
0x73ABE5E8: found const array DES_sbox6 (used in DES)
0x73ABE628: found const array DES_sbox7 (used in DES)
0x73ABE6A8: found const array DES_pc1 (used in DES)
0x73ABE6E0: found const array DES_pc2 (used in DES)
```

ひとつ目の異常

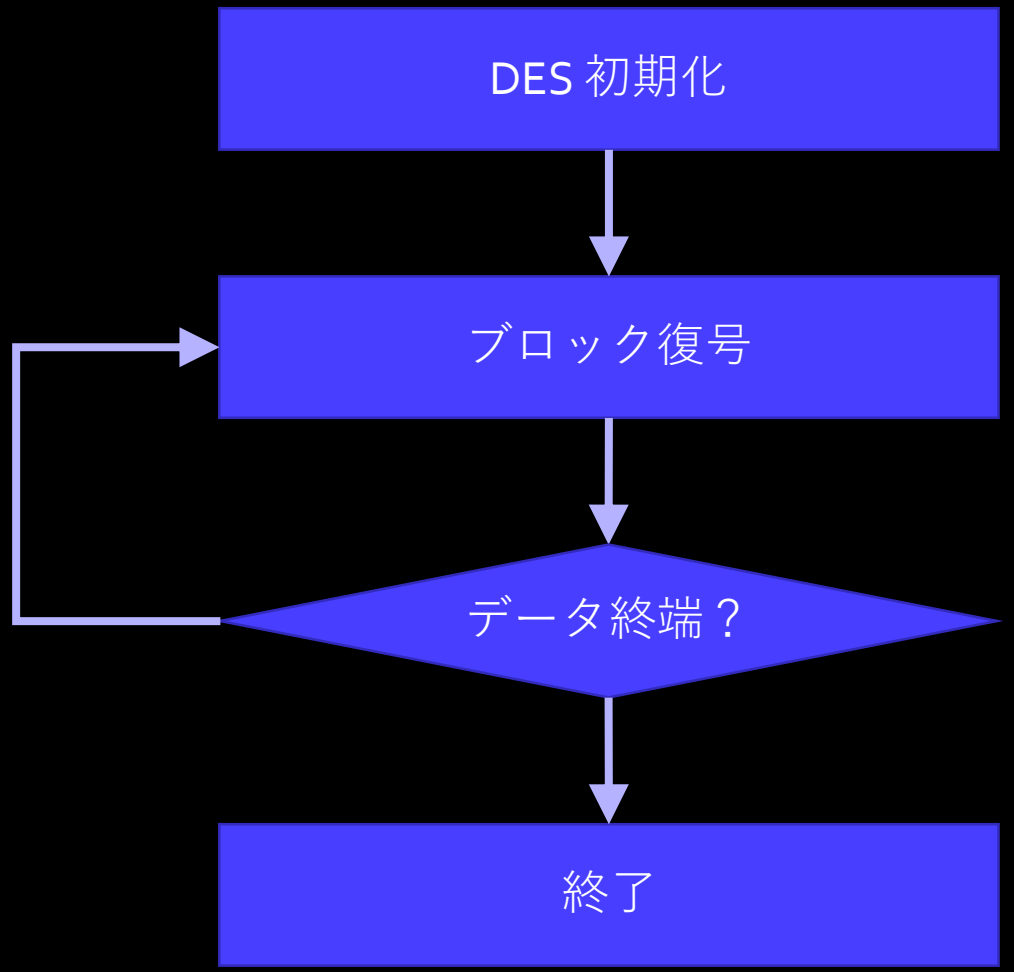
独自の DES Sbox

sbox1	14, 4, 13, 1, 1, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7, 0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8, 4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0, 15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13
sbox2	15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10, 3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5, 0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15, 13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9
sbox3	10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8, 13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1, 13, 6, 4, 9, 8, 15, 3, 0, 11, 1, 2, 12, 5, 10, 14, 7, 1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3, 11, 5, 2, 12
sbox4	7, 13, 14, 3, 0, 6, … 4, 7, 2, 12, 1, 10, 14, 9, 10, 6, 9, 0, 12, 11, … 9, 4, 5, 11, 12, 7, 2, 14
sbox5	2, 12, 4, 1, 7, 10, … 5, 0, 15, 10, 3, 9, 8, 6, 4, 2, 1, 11, 10, 13, … 6, 15, 0, 9, 10, 4, 5, 3
sbox6	12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11, 10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8, 9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6, 4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13
sbox7	4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1, 13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6, 1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2, 6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12
sbox8	13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 13, 14, 5, 0, 12, 7, 1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2, 7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8, 2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11

sbox 1, sbox8 が標準と異なる

ふたつ目の異常

DES 暗号鍵のリセット



入力された暗号鍵から Subkeys を作成

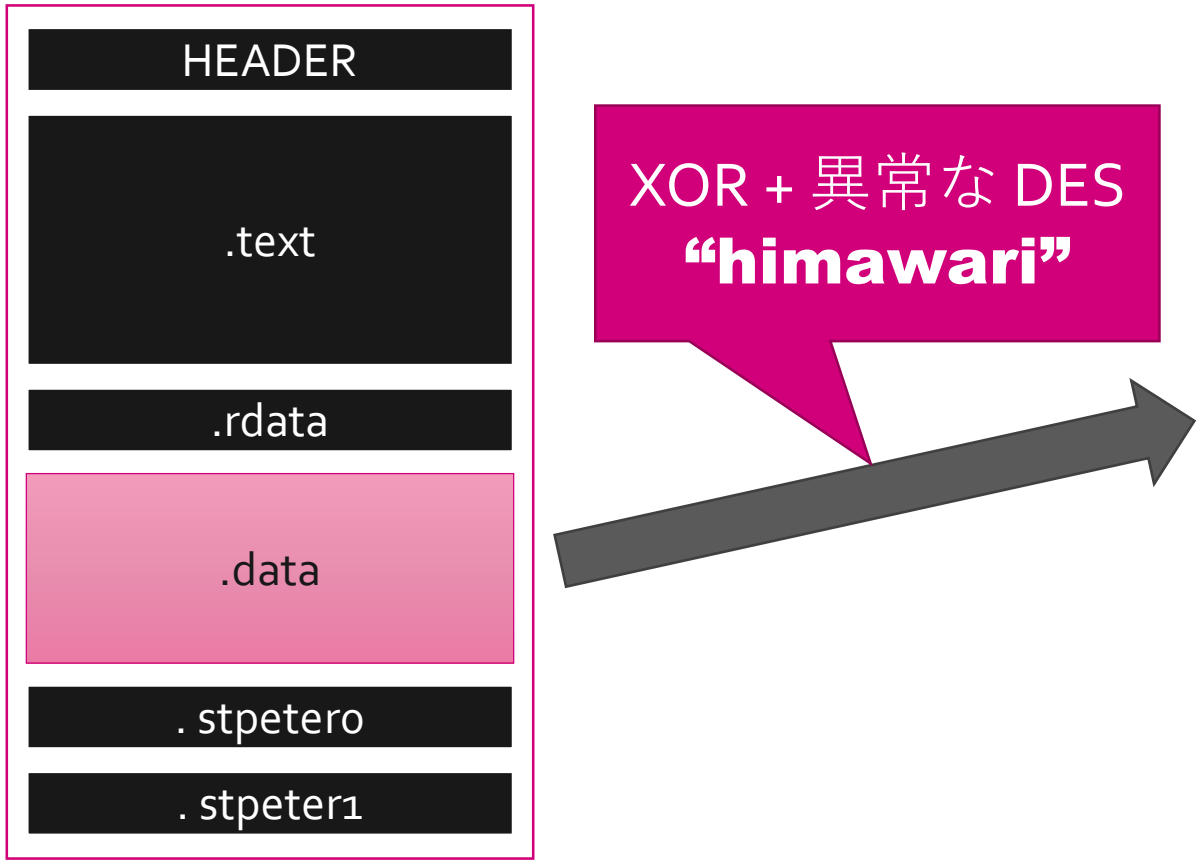
8バイトのデータを復号

一時データのクリーンアップ

Subkeys のデータも初期化するため、
暗号鍵が “\xoo” * 8 の場合と同じ状態になる

設定データの復号

XOR + 異常な DES

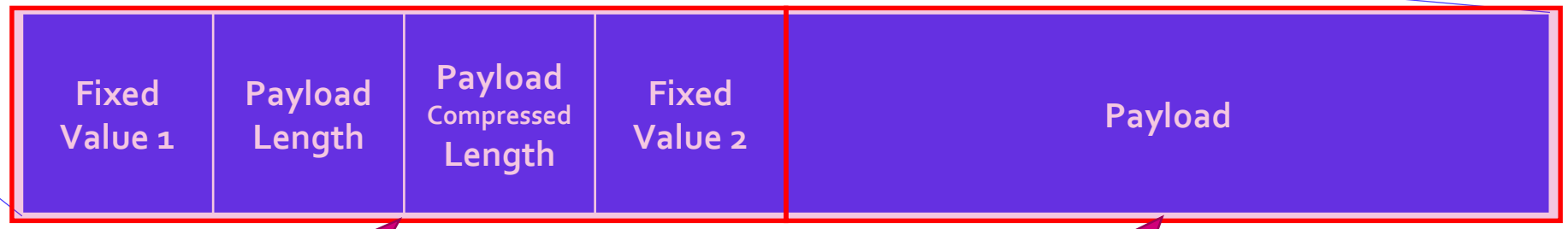


通信データの復号（HTTP）

AES, zlib + XOR + 異常な DES

```
POST /HWW8l3q1/index.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; W
3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0
Content-Length: 97
Host: ducksow.ddnsgeek.com:443

.)....jX..C/=qk8x..@......"..17..E@....]. j..b.u
```



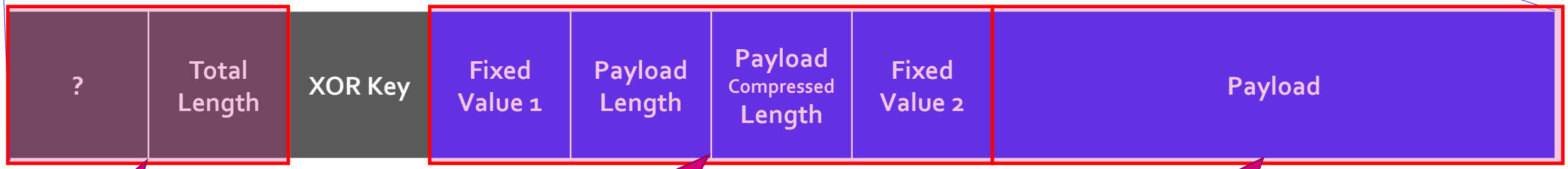
AES
設定データ内の暗号鍵

zlib + XOR + 異常な DES
設定データ内の暗号鍵

通信データの復号（独自）

XOR, AES, zlib + XOR + 異常な DES

```
....*...N....)....jX..C/=qk8x..@......"..17..E@....]. j..b.......
+...J...o0.M.Mf.@.m.m......).A.|.7f....'T{....
```



XOR
XOR Key

AES
設定データ内の暗号鍵

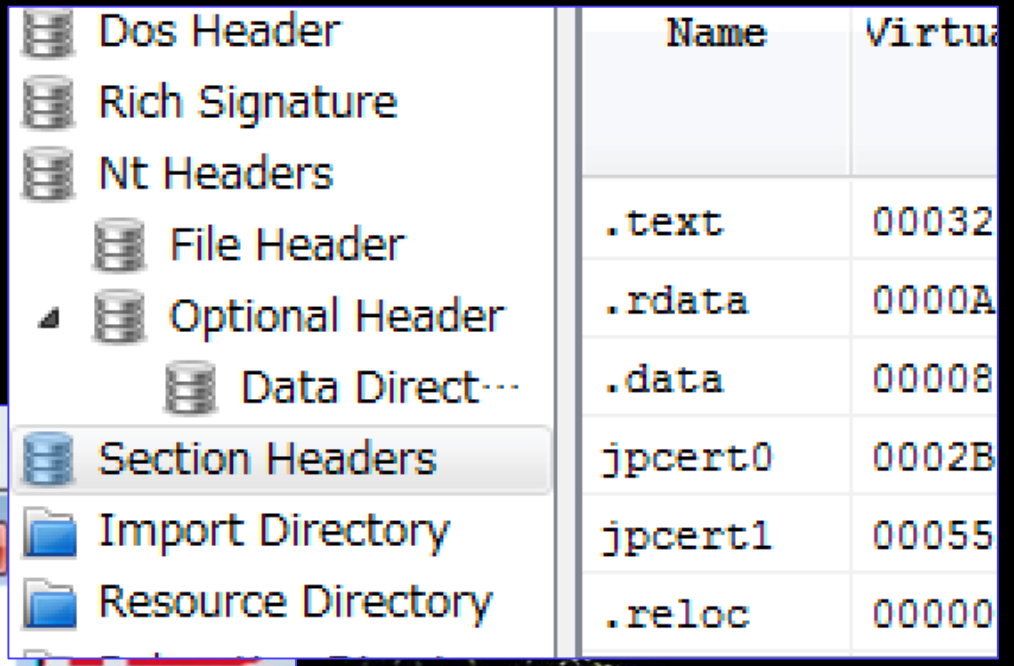
zlib + XOR + 異常な DES
設定データ内の暗号鍵

Lavender?

2018年1月にサブミットされた検体

```
lea     eax, [ebp+var_380]
push    eax
push    370h
mov     edi, offset encrypted_config
push    edi
mov     [ebp+var_10], 'EVAL'
mov     [ebp+var_C], 'REDN'
mov     [ebp+var_8
call    aa_DES_pro
add     esp, 20h
push    hHandle
```

https://www.hybrid-analysis.com/sample/db7c1534dede15be08e651784d3a5d2ae41963d192b0f8776701b4b72240c38d?environmentId=100

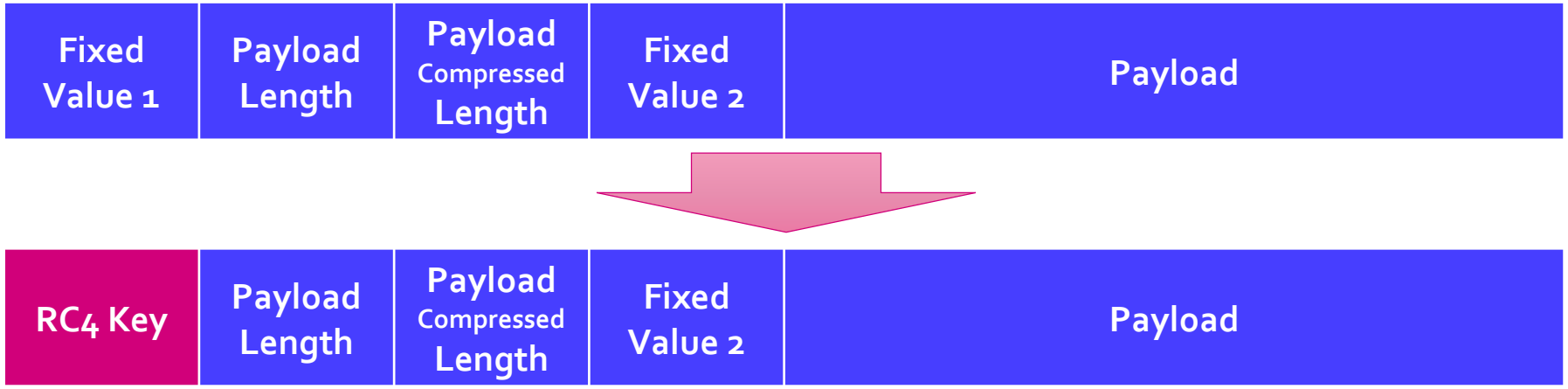


Secureworks

Lavender における変化

異常な DES のみに変更

- 設定データ
  - XOR が無くなり異常な DES のみに
  - 暗号鍵は LAVENDER
- 通信
  - XOR が無くなり RC4 を使用する
  - RC4 の暗号鍵はデータヘッダの先頭に格納



暗号化されたデータの復号

ファイルの復号

単純な XOR + AES 復号

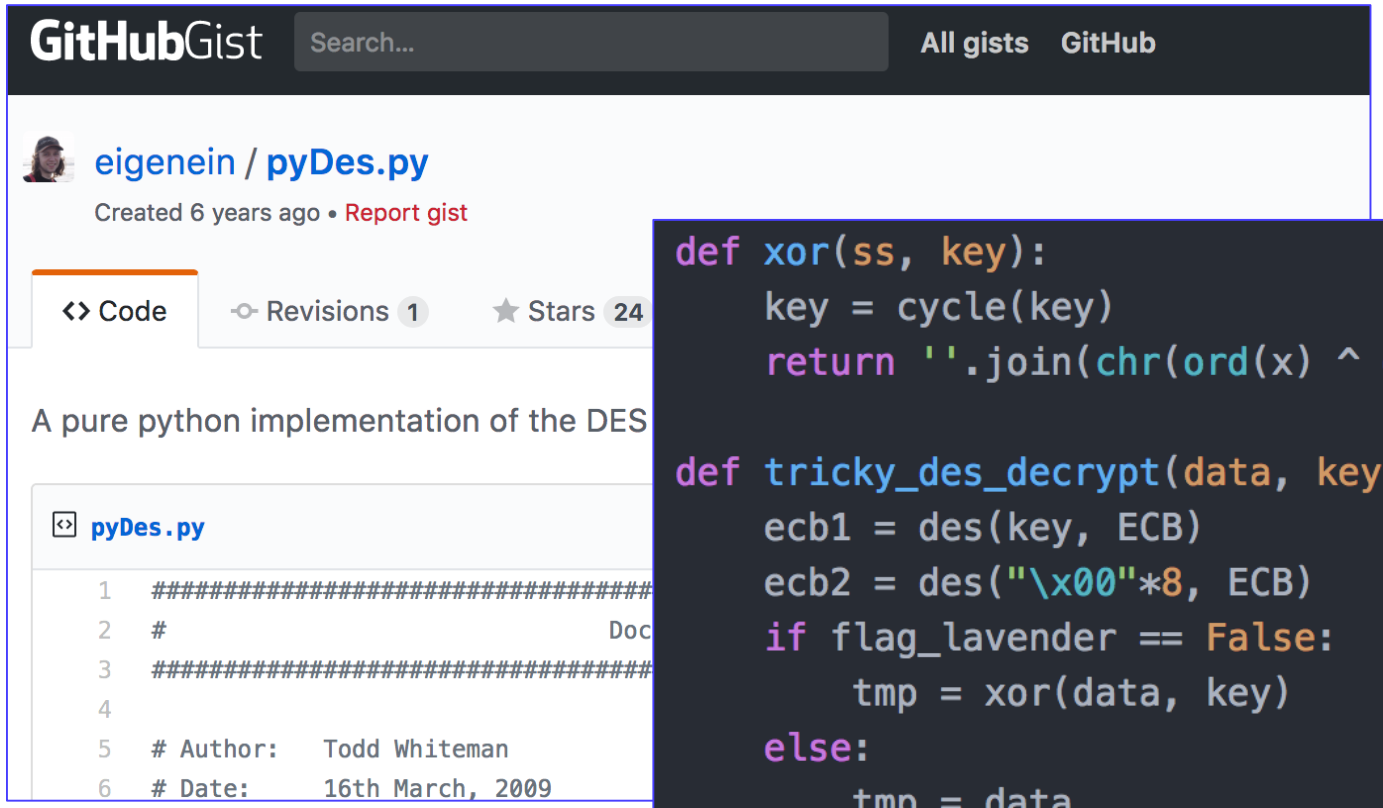
```
enc = data[enc_offset:enc_offset+enc_size]
dec = ""
for c in enc:
    dec += chr(ord(c) ^ args.xor_key)
out_file = root + "_" + filename
fp = open(out_file, "wb")
fp.write(dec)
fp.close()
print("[*] save decoded data as %s" % out_file)
if os.path.splitext(filename)[1] != ".exe" and os.path
    decrypt_binary(out_file)
```

```
def decrypt_binary(target_file):
    fp = open(target_file, "rb")
    enc = fp.read()
    fp.close()

    aes = AES.new(args.aes_key)
    dec = aes.decrypt(enc)
    root, ext = os.path.splitext(target_file)
    out_file = root + "_dec.bin"
    fp = open(out_file, "wb")
    fp.write(dec)
    fp.close()
    print("[*] save decrypted data as %s" % out_file)
```

異常な DES の実装

sbox の変更 + 暗号鍵のリセット



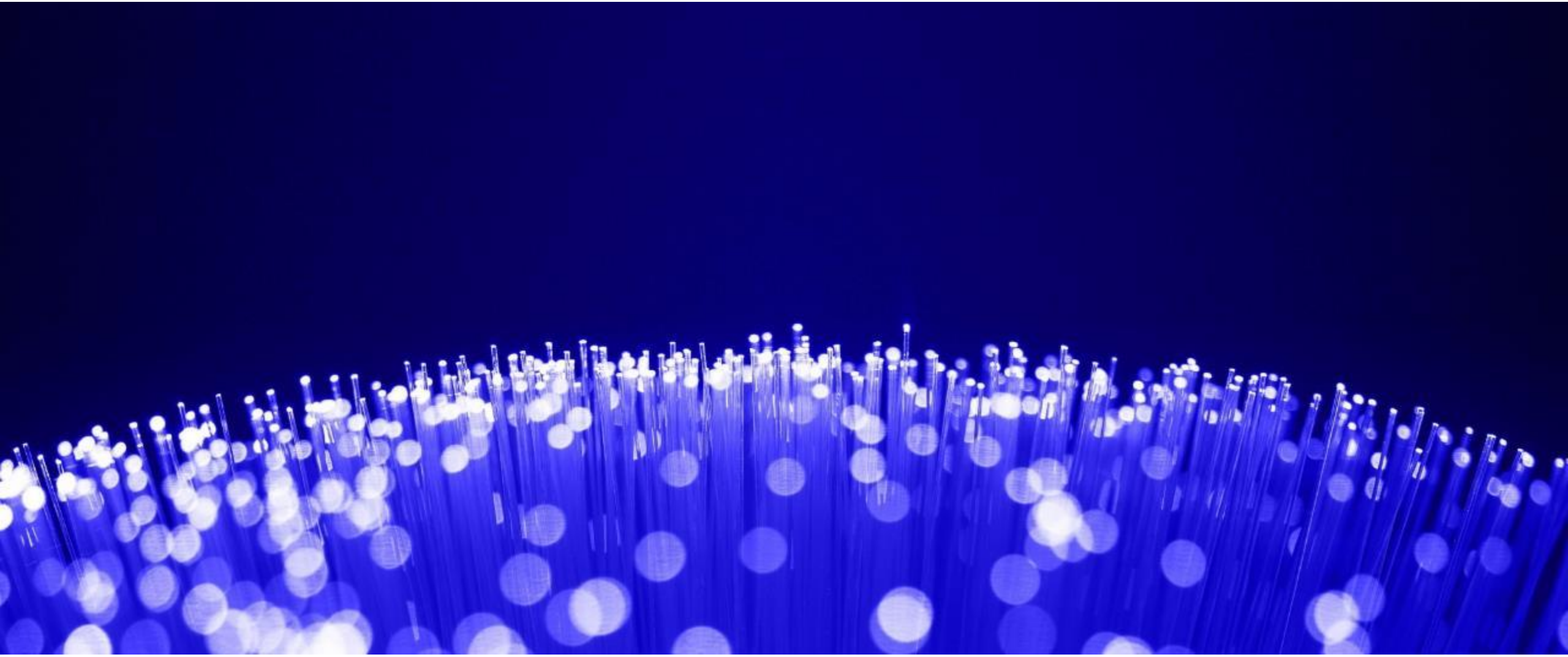
https://gist.github.com/eigenein/1275094

```python
def xor(ss, key):
    key = cycle(key)
    return ''.join(chr(ord(x) ^ ord(y)) for (x,y) in izip(ss, key))

def tricky_des_decrypt(data, key, flag_lavender):
    ecb1 = des(key, ECB)
    ecb2 = des("\x00"*8, ECB)
    if flag_lavender == False:
        tmp = xor(data, key)
    else:
        tmp = data
    dec = ecb1.decrypt(tmp[0:8])
    dec += ecb2.decrypt(tmp[8:])
    return dec
```

デモ

参考情報



参考 URL

- オープンソースのRATを改良したマルウエアRedLeaves(2017-04-03)
  - https://www.jpcert.or.jp/magazine/acreport-redleaves.html
- Cyber espionage warning
  - https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/april/cyber-espionage-warning/
- 「ChChes」を操る標的型サイバー攻撃キャンペーン「ChessMaster」による諜報活動の手口 | トレンドマイクロ セキュリティブログ
  - http://blog.trendmicro.co.jp/archives/15551
- セキュリティ研究センターブログ: 防衛関連のファイルを装うマクロマルウェアの新しい手口
  - http://blog.macnica.net/blog/2017/12/post-8c22.html
- マルウエアRedLeavesを検知するVolatility Plugin(2017-05-02)
  - https://www.jpcert.or.jp/magazine/acreport-redleaves2.html
- A pure python implementation of the DES and TRIPLE DES encryption algorithms
  - https://gist.github.com/eigenein/1275094
- ida/idapython_tools/findcrypt at master · you0708/ida
  - https://github.com/you0708/ida/tree/master/idapython_tools/findcrypt


Secureworks®