MWS Cup 2015
課題 2 紹介

2015/10/21

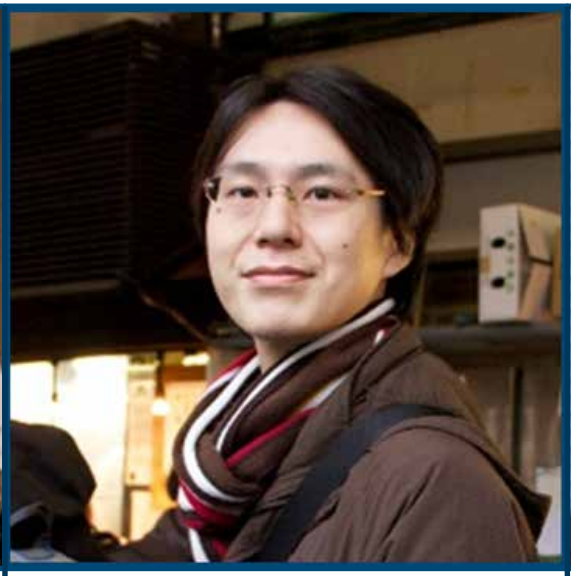
JPCERT/CC **分析センター**

中津留 勇

課題 2 作成委員会

中津留 勇

- JPCERT/CC



羽田 大樹

- NTT コムセキュリティ

大坪 雄平

- 警察庁
- NISC

課題 2 のテーマ

yuhei0320 10:00 AM

emdiviのコマンド一覧や接続先URLの難読化された文字列を復号している部分の解析は割と手頃な印象を受けています。問１：指定した文字列を復号せよ。問２：復号のアルゴリズムから、暗号化のアルゴリズムを類推し、問題作成者が指定する文字列を暗号化せよ。みたいな問題だと、時間内でできますし、採点もしやすいかと。ポイントは問１は動的解析でもできるけど、問２は静的解析を行わないと出来ないということです。問１の成果は問２の検算にも使えます。

you0708 10:30 AM

おー。いい感じですね。カスペルスキーがめっちゃブログに書いてた気がするので要確認ですね

Emdivi に関連した攻撃

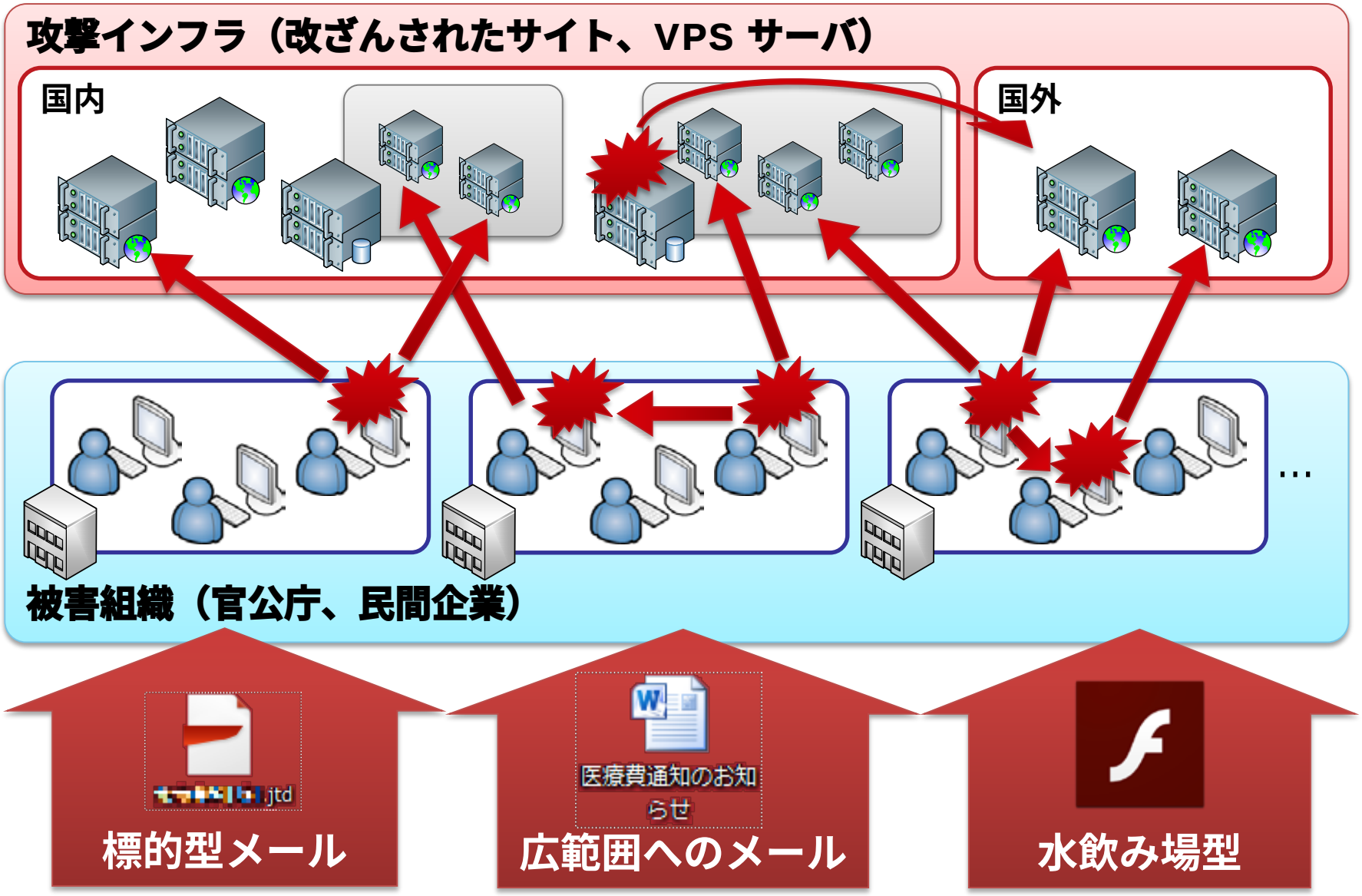
- JPCERT/CC の高度サイバー攻撃対応（2015/04-09）

130組織

Emdivi 関連

93組織

Emdivi に関連した攻撃



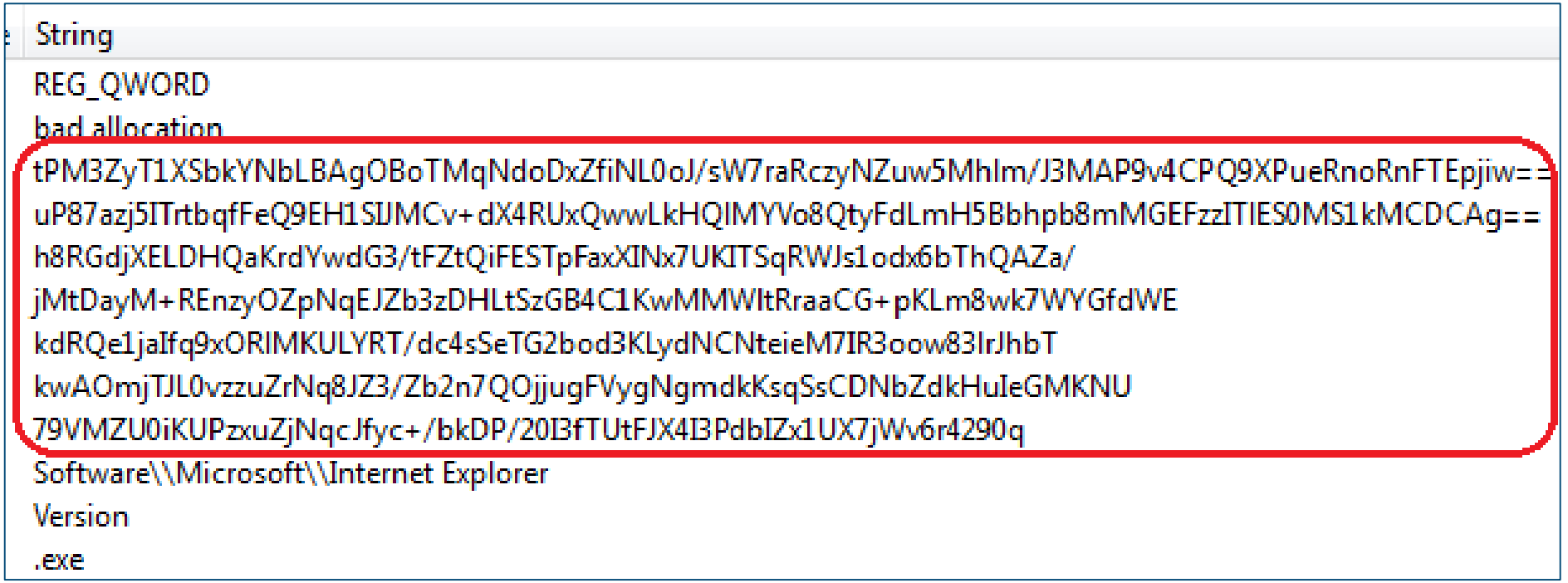
課題 2

- Emdivi の静的解析データ（IDA データベース形式）

1. 特定の関数の機能特定
2. 暗号アルゴリズムの推定
3. 復号処理の実装

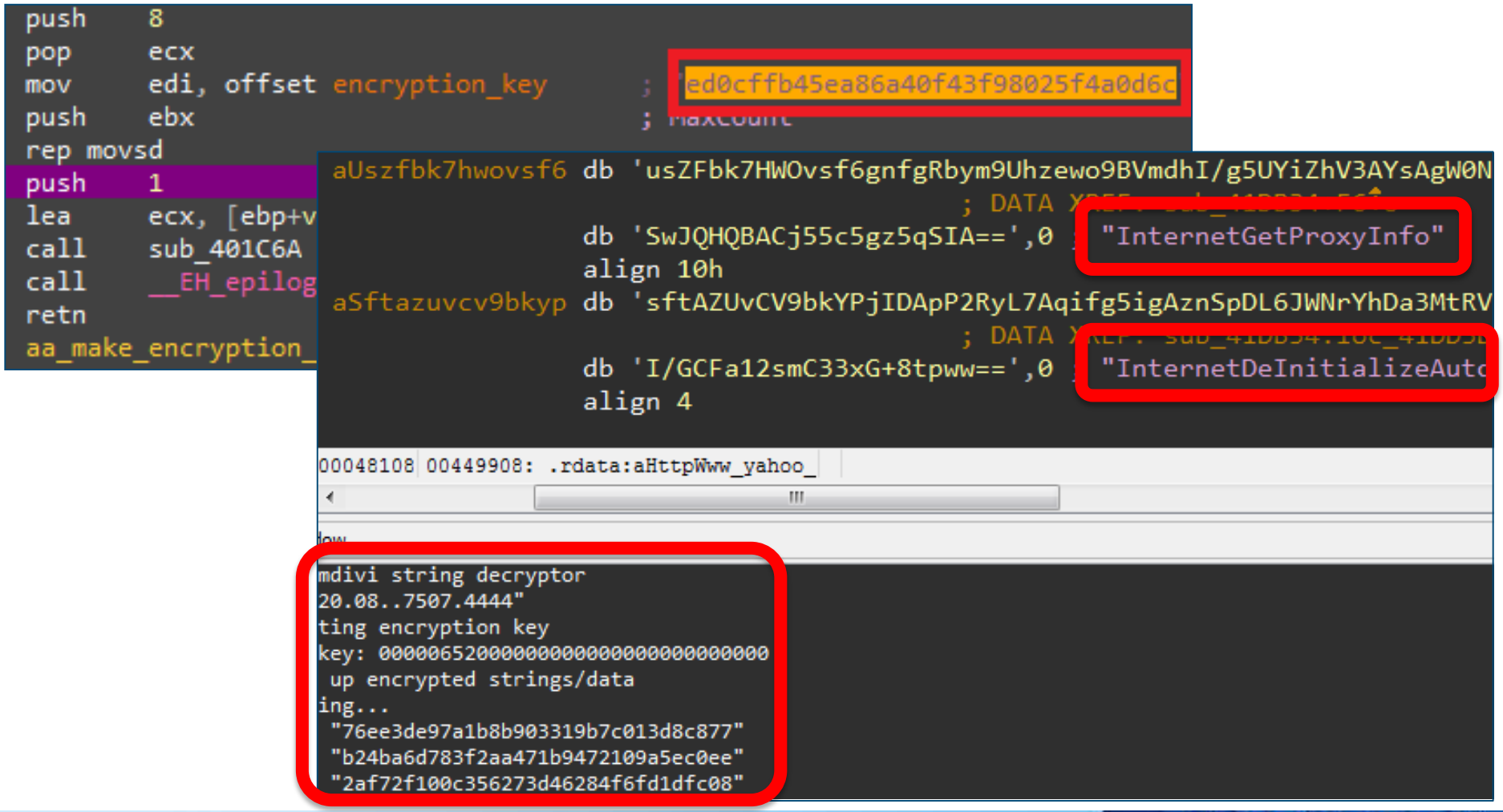
暗号化された文字列

- **検体内部で使用される文字列**
  - —URL、コマンド、ファイルパス、レジストリエントリ名



復号とインシデント対応

- 暗号処理を解析して文字列を復号し、インシデント対応に活用



復号処理の実装

c2_script_template.py

```
1  import struct
2
3  key = "c09741de703aab051b3fa79c56a8caec".decode("hex")
4  enc_str = "HXemdsWgm/4L2NUlEWM4R4rMtsCl/7V8cjMRpV9romY=".decode("base64")
5
6  def mask32bit(input_dword):
7      return input_dword & 0xffffffff
8
9  def decrypt(key, input_str):
10     input_dword = [struct.unpack("<I", input_str[i:i+4])[0] for i in range(0, len
11     key_dword = struct.unpack(">4I", key)
12
13     # insert decryption process here!
14
15     out = "".join([struct.pack("<I", input_dword[i]) for i in range(len(input_dwor
16     return out
17
18 def emdivi_decrypt(key, input_str):
19     dec = decrypt(key, input_str)
20
```

解答は CODE BLUE 2015 で！！

朝長 秀誠 & 中村 祐

Shusei Tomonaga & Yuu Nakamura

朝長 秀誠

一般社団法人JPCERTコーディネーションセンター 分析センター所属 外資系ITベンダーでのセキュリティ監視・分析業務を経て、2012年12月から現職。現在は、マルウェア分析・フォレンジック調査に従事。主に、標的型攻撃に関するインシデント分析を行っている。

中村 祐

一般社団法人JPCERTコーディネーションセンター 分析センター所属
大手ポータルサイトでの運用業務を経て、2012年4月から現職。現在は、主に改ざんされたWebサイトの分析やマルウェア分析などに従事。また最近では、標的型攻撃に関連するマルウェアの分析にも力を入れている。

[APT][Reverse engineering]

日本の組織をターゲットにした攻撃キャンペーンの詳細

近年日本国内で標的型攻撃の被害にあう組織が増加している。しかし、このような攻撃の詳細が明らかになることは少ない。JPCERT/CCでは、日本国内の組織を狙う複数の攻撃キャンペーンに関し

分かってほしいこと

- マルウェアを理解するということ
- マルウェア解析をする仕事

ありがとうございました

連絡先

- aa-info@jpcert.or.jp
- https://www.jpcert.or.jp

インシデント報告

- info@jpcert.or.jp
- https://www.jpcert.or.jp/form/