

MWS Cup 2015

課題 2 紹介

2015/10/21

JPCERT/CC 分析センター

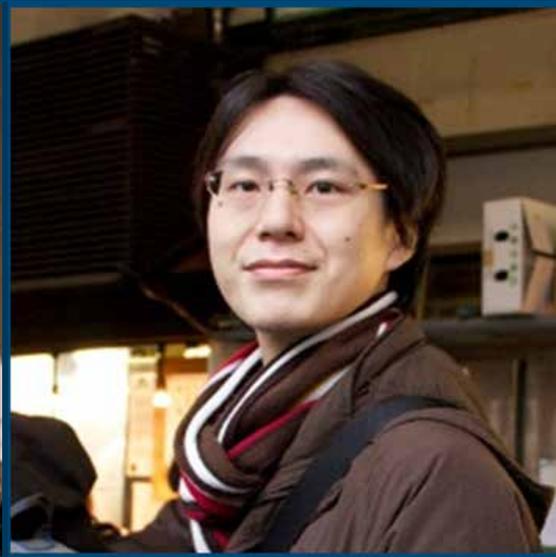
中津留 勇

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)

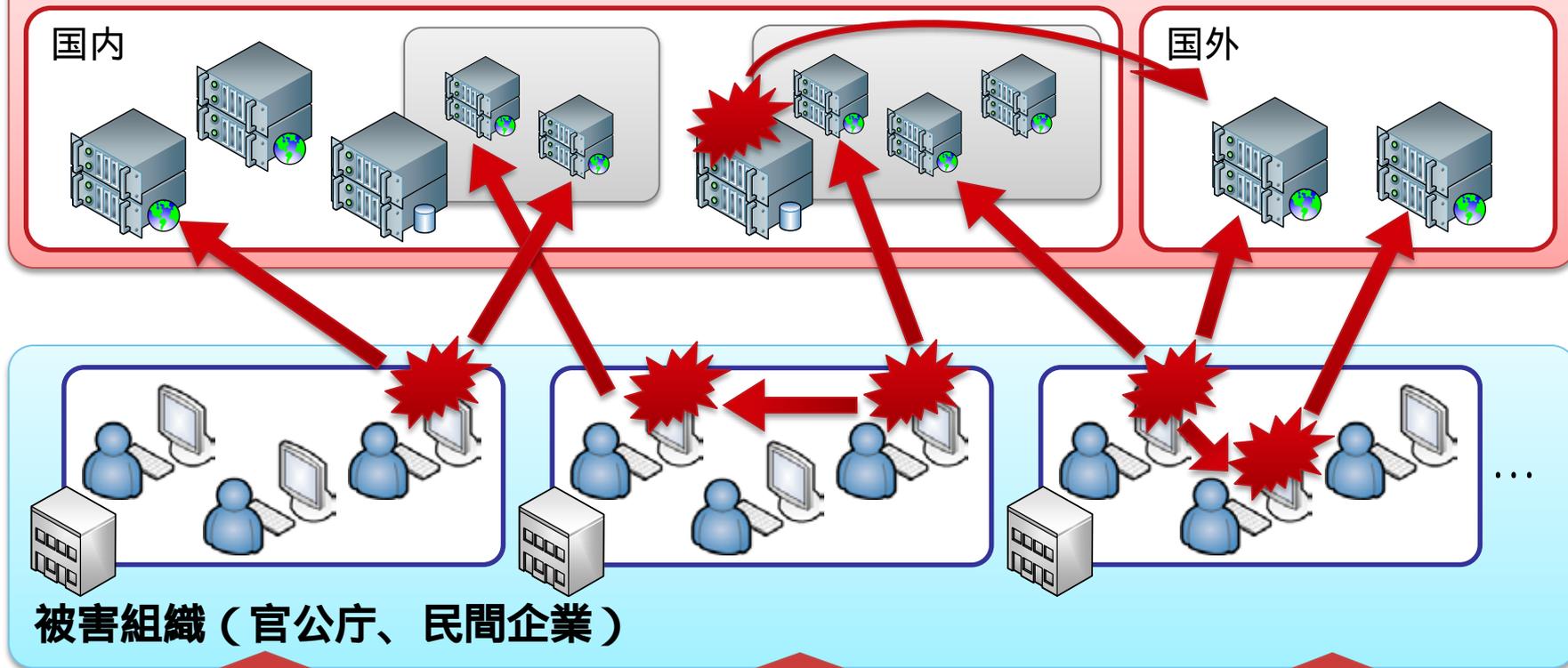
130 組織

Emdivi 関連

93 組織

Emdivi に関連した攻撃

攻撃インフラ（改ざんされたサイト、VPS サーバ）



標的型メール



医療費通知のお知らせ

広範囲へのメール



水飲み場型

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

```
String
REG_QWORD
bad allocation
tPM3ZyT1XSbkYnBLBAgOBoTMqNdoDxZfiNL0oJ/sW7raRczyNZuw5MhIm/J3MAP9v4CPQ9XPueRnoRnFTEpjiw==
uP87azj5ITrtbqfFeQ9EH1SJMcv+dX4RUxQwwLkHQIMYVo8QtyFdLmH5Bbhpb8mMGEFzzITIES0MS1kMCDCAg==
h8RGdjXELDHQaKrdYwdG3/tFZtQiFESTpFaxXINx7UKITSqRWJs1odx6bThQAza/
jMtDayM+REnzyOZpNqEJZb3zDHLtSzGB4C1KwMMWItRraaCG+pKLM8wk7WYGfdWE
kdRQe1jaIfq9xORIMKULYRT/dc4sSeTG2bod3KLydNCNteieM7IR3oow83lrJhbT
kwAOmjTJL0vzzuZrNq8JZ3/Zb2n7QOjjugFVygNgmdkKsqSsCDNbZdkHuIeGMKNU
79VMZU0iKUPzXuZjNqcJfyc+/bkDP/20BfTUtFJX4BpDbIZx1UX7jWv6r4290q
Software\\Microsoft\\Internet Explorer
Version
.exe
```

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

```
push 8
pop ecx
mov edi, offset encryption_key ; ed0cfb45ea86a40f43f98025f4a0d6c
push ebx ; maxCount
rep movsd
push 1
lea ecx, [ebp+v
call sub_401C6A
call __EH_epilog
retn
aa_make_encryption_

aUzsfbk7hwovsf6 db 'usZFbk7HW0vsf6gnfgrbym9Uhzewo9BVmdhI/g5UYiZhV3AYsAgW0N
; DATA XREF: sub_410034+56
"InternetGetProxyInfo"
db 'SwJQHQBACj55c5gz5qSIA==',0
align 10h
aSftazuv cv9bkyp db 'sftAZUvCV9bkYPjIDApP2RyL7Aqifg5igAznSpDL6JWnrYhDa3MtRV
; DATA XREF: sub_410034+10C+410034
"IInternetDeInitializeAuto
db 'I/GCFa12smC33xG+8tpww==',0
align 4

00048108|00449908: .rdata:aHttpWww_yahoo_
<
low
mdivi string decryptor
20.08..7507.4444"
ting encryption key
key: 00000652000000000000000000000000
up encrypted strings/data
ing...
"76ee3de97a1b8b903319b7c013d8c877"
"b24ba6d783f2aa471b9472109a5ec0ee"
"2af72f100c356273d46284f6fd1dfc08"
```

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(input_str), 4)]
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_dword))]
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/>