MWS Cup 2016
課題2: 静的解析

中津留 勇

2016/10/11

課題2 担当

中津留　勇

- SecureWorks Japan 株式会社

稲垣　俊

- セコム株式会社

課題2 の変わらぬテーマ

- 静的解析を通じ

マルウェアを正しく理解する

最新情報を得る

実務に近い作業

MWS Cup 2015 課題2 振り返り

SecureWorks
A Dell Company

Emdivi

- 日本における大規模な標的型攻撃で使用された検体の解析

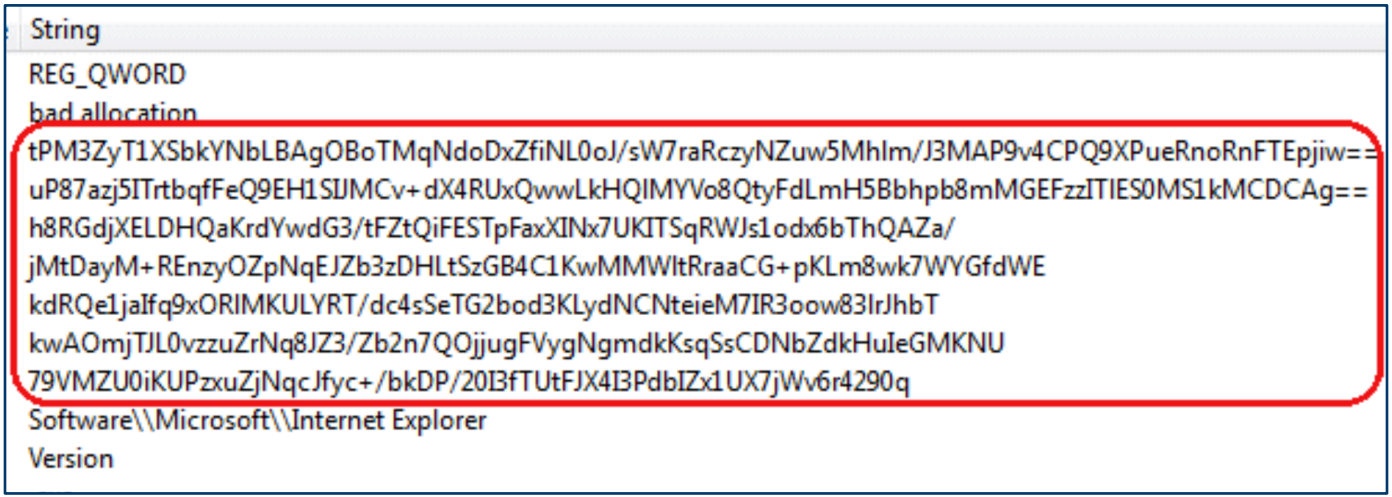
1．特定の関数の機能特定

2．暗号アルゴリズムの推定

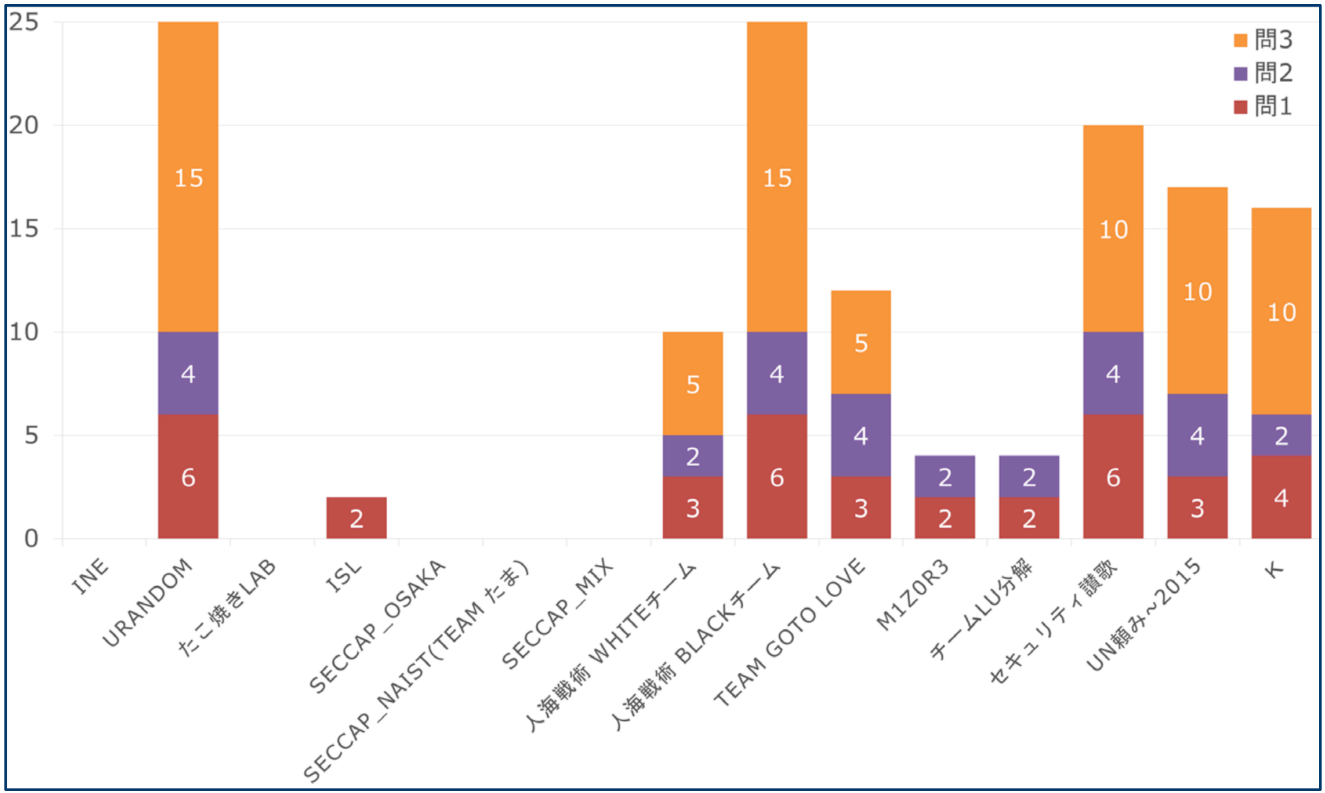
3．復号処理の実装

Emdivi とインシデント対応

- 暗号化された文字列を復号し、接続先 URL などの情報を得る



課題2 採点結果



課題2 の反省

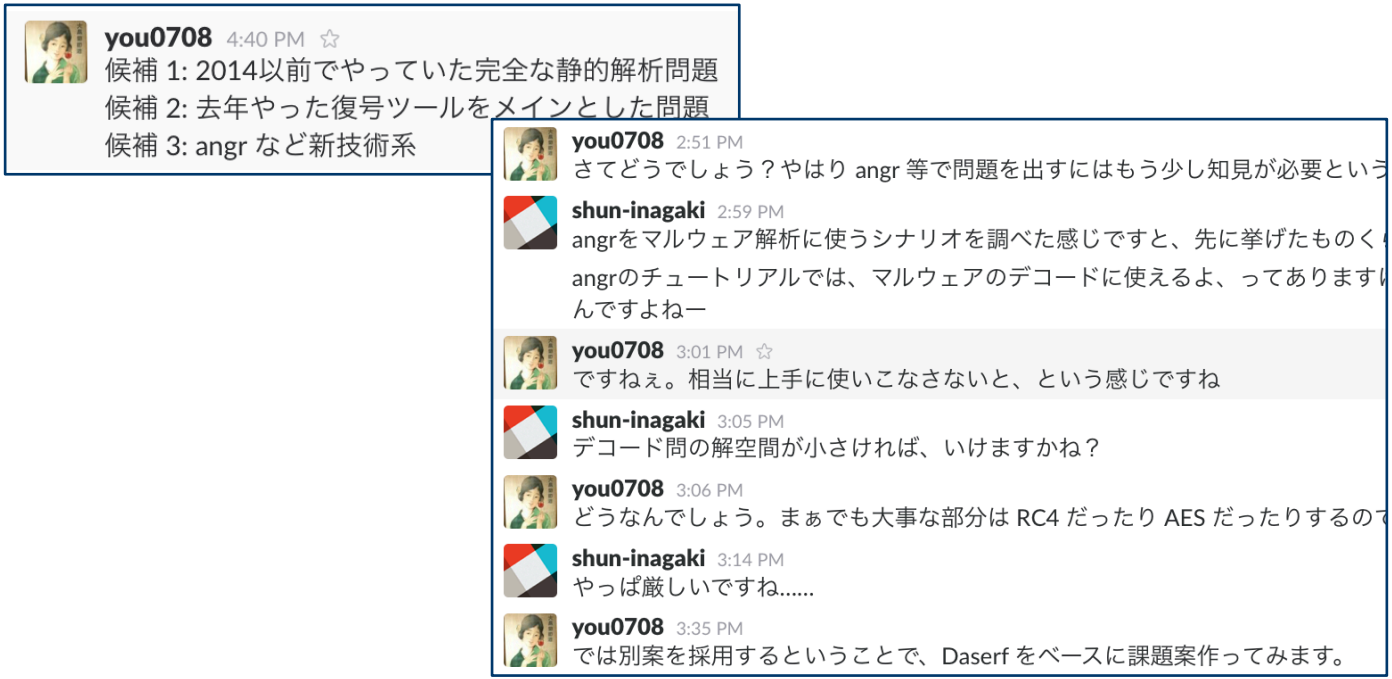
0 か 1 か問題

- 問題数が少ない
- 段階的な問題が無い
  - あっさりと諦める


MWS Cup
2016
課題2
SecureWorks
A Dell Company

課題2 どうしよう

- 昨年を踏襲 or 新技術



Tick/Daserf

- 日本国内で数年前から発生していた標的型攻撃

http://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

標的型攻撃に用いられるマルウェア、Daserf とは

Daserf はバックドア機能を有するマルウェアで、Nioupale とも呼ばれています。Daserf については、2016 年 5 月に Symantec がブログ[ii]で報告していますが、それまではセキュリティベンダによる報告はほとんどなく、このマルウェアの存在自体、広く知られているとは言えない状況でした。一方、ラックは 2013 年 1 月頃以降に対応した複数の標的型攻撃事案において Daserf を確認しており、これらの分析を続けてきました。その結果、Daserf が日本の重要インフラを標的とした攻撃者に使用され、長期間にわたって標的組織に潜伏しつつ活動している可能性が高いことが明らかになりました。

図 1 は、ラックが対応した事案において Daserf が使われた業種を分類したグラフです。グラフ外周右側の枠に含まれるのが重要インフラに属する業種[iii]で、56%と過半数を占めていることがわかります。外周左側の枠は重要インフラで利用される機器を製造する事業者で、これらを含めるとすべての事案が重要インフラに直接的、間接的に関連していることがわかります。このことから、Daserf を使う攻撃者は、少なくとも日本においては重要インフラやその関連企業をターゲットとしている可能性が高いと考えられます。

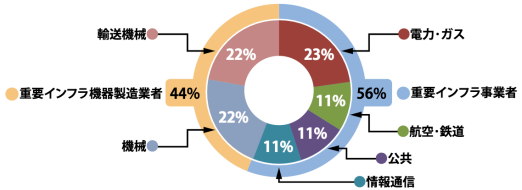


図 1 ラックが対応した標的型攻撃事案のターゲット組織

http://www.lac.co.jp/security/report/pdf/20160802_cgview_vol2_a001t.pdf

課題2

1．コード難読化

2．暗号アルゴリズム（選択式）

3．暗号化/エンコード処理

4．暗号化されたデータの復号

5．設定情報の調査

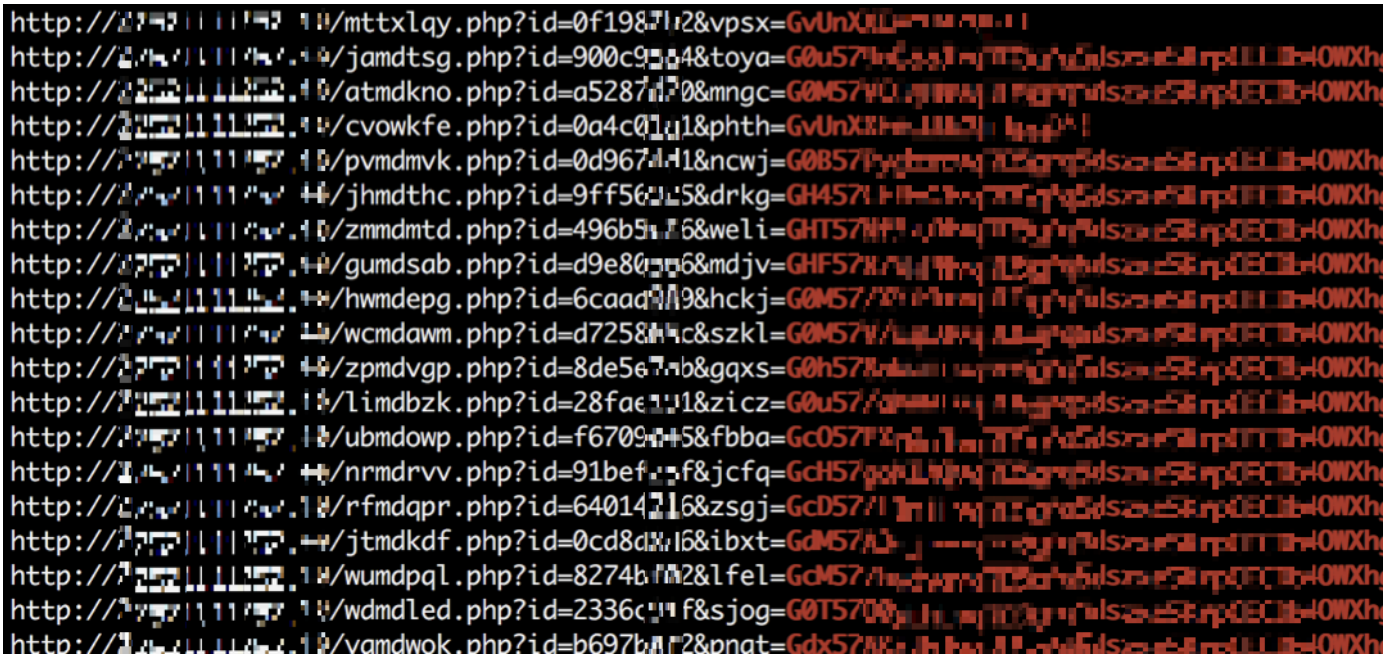
暗号アルゴリズム

- AES, DES, 3DES, RC4, TEA?

```
CODE:004198B0 120                jl      loc_419955
CODE:004198B6 120                inc     eax
CODE:004198B7 120                mov     [ebp+var_18], eax
CODE:004198BA 120                mov     [ebp+var_10], 0
CODE:004198C1
CODE:004198C1     loc_4198C1:                                ; CODE XREF: sub_41
CODE:004198C1 120                inc     [ebp+var_1A]
CODE:004198C4 120                xor     eax, eax
CODE:004198C6 120                mov     al, [ebp+var_1A]
CODE:004198C9 120                mov     al, [ebp+eax+var_11A]
CODE:004198D0 120                mov     [ebp+var_11], al
CODE:004198D3 120                mov     al, [ebp+var_11]
CODE:004198D6 120                add     [ebp+var_19], al
CODE:004198D9 120                xor     eax, eax
CODE:004198DB 120                mov     al, [ebp+var_19]
CODE:004198DE 120                mov     al, [ebp+eax+var_11A]
CODE:004198E5 120                xor     edx, edx
CODE:004198E7 120                mov     dl, [ebp+var_1A]
CODE:004198EA 120                mov     [ebp+edx+var_11A], al
CODE:004198F1 120                xor     eax, eax
CODE:004198F3 120                mov     al, [ebp+var_19]
CODE:004198F6 120                mov     dl, [ebp+var_11]
```

暗号化されたデータ

- Daserf が実行したコマンドの結果



設定情報

- 格納先、暗号/エンコード方式

```
004188AB 968                call    CreateFileA
004188B0 94C                mov     [ebp+hFile], eax
004188B3 94C                cmp     [ebp+hFile], 0FFFFFFFFh
004188B7 94C                jz      loc_418B39
004188BD 94C                push    2                   ; dwMoveMethod
004188BF 950                push    0                   ; lpDistanceToMoveHigh
004188C1 954                push    0FFFFFE16h          ; lDistanceToMove
004188C6 958                mov     eax, [ebp+hFile]
004188C9 958                push    eax                 ; hFile
004188CA 95C                call    SetFilePointer
004188CF 94C                lea     eax, [ebp+Buffer] ; void *
004188D5 94C                mov     edx, 80h            ; unsigned int
004188DA 94C                call    Windows::ZeroMemory(void *,uint)
004188DF 94C                push    0                   ; lpOverlapped
004188E1 950                lea     eax, [ebp+NumberOfBytesRead]
004188E4 950                push    eax                 ; lpNumberOfBytesRead
004188E5 954                push    18h                 ; nNumberOfBytesToRead
004188E7 958                lea     eax, [ebp+Buffer]
004188ED 958                push    eax                 ; lpBuffer
004188EE 95C                mov     eax, [ebp+hFile]
```

Re: 課題2のテーマ

マルウェアを正しく理解する

最新情報を得る

実務に近い作業


Thank you!
SecureWorks
A Dell Company