

MWS Cup 2016

課題2: 静的解析

中津留 勇

2016/10/11

課題2 担当



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

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

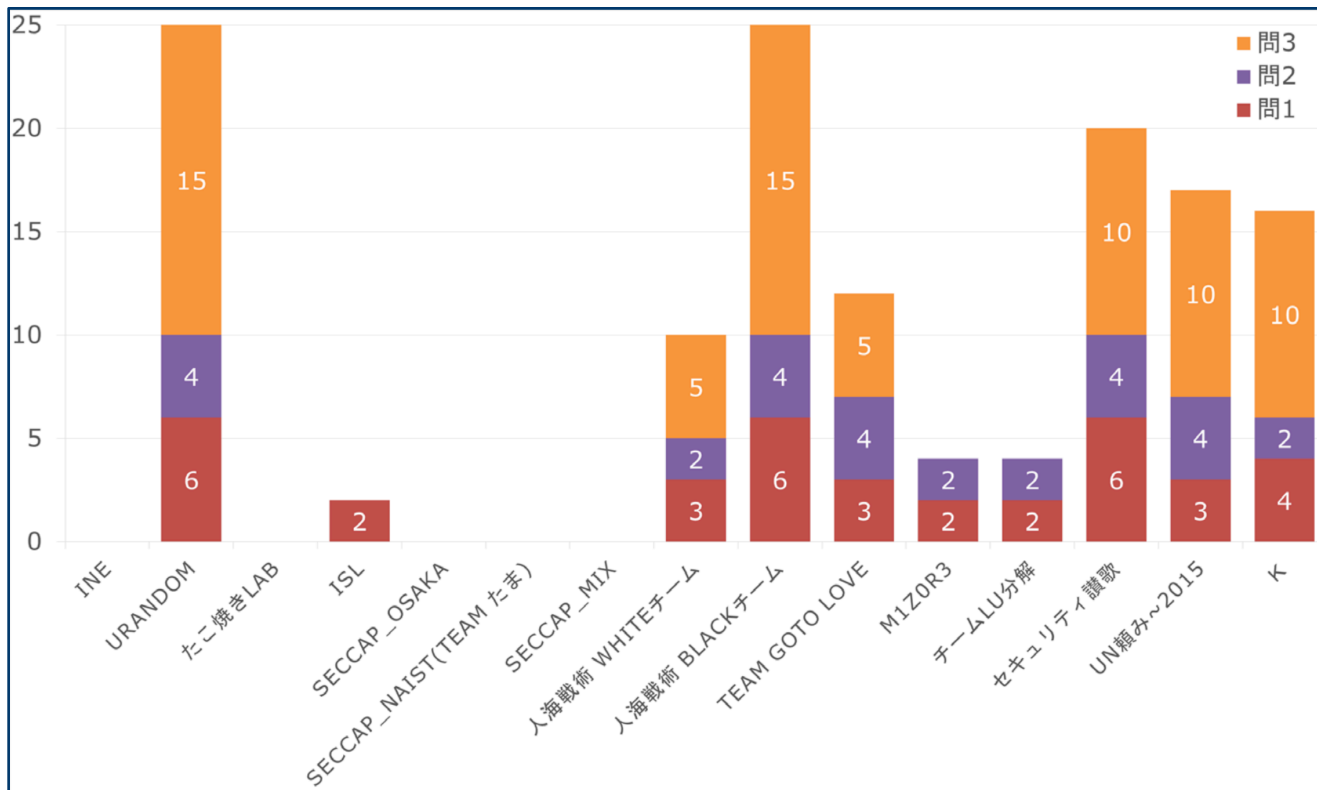
3. 復号処理の実装

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

```
String
REG_QWORD
bad allocation
tPM3ZyT1XSbkYNbLBAgOBoTMqNdoDxZfiNL0oJ/sW7raRczyNZuw5Mhlm/J3MAP9v4CPQ9XPueRnoRnFTepjiw==
uP87azj5ITrtbqfFeQ9EH1SIJMCv+ dx4RUxQwwLkHQIMYVo8QtyFdLmH5Bbhhpb8mMGEFzzITIES0MS1kMCDCAg==
h8RGdjXELDHQaKrdYwdG3/tFZtQiFESTpFaxXINx7UKITSqRWJs1odx6bThQAZa/
jMtDayM+REnzyOZpNqEJZb3zDHlTszGB4C1KwMMWltRraaCG+ pKLm8wk7WYGfdWE
kdRQe1jaIfq9xORIMKULYRT/dc4sSeTG2bod3KLydNCNteieM7IR3oow83lrJhbT
kwAOmjTJL0vzzuZrNq8JZ3/Zb2n7QOjjugFVygNgmdkKsqSsCDNbZdkHuIeGMKNU
79VMZU0iKUPzXuZjNqcJfyc+/bkDP/20BftUtFJX4BPdbIZx1UX7jWv6r4290q
Software\\Microsoft\\Internet Explorer
Version
```

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

A nighttime photograph of a city street, likely in New York City, featuring light trails from traffic and illuminated buildings. A semi-transparent blue overlay covers the left side of the image, containing the title text.

MWS Cup 2016 課題2

課題2 どうしよう

• 昨年を踏襲 or 新技術



you0708 4:40 PM ☆

候補 1: 2014以前でやっていた完全な静的解析問題

候補 2: 去年やった復号ツールをメインとした問題

候補 3: angr など新技術系



you0708 2:51 PM

さてどうでしょう？やはり angr 等で問題を出すにはもう少し知見が必要という



shun-inagaki 2:59 PM

angrをマルウェア解析に使うシナリオを調べた感じだと、先に挙げたものくら
angrのチュートリアルでは、マルウェアのデコードに使えるよ、ってあります
んですよー



you0708 3:01 PM ☆

ですねえ。相当に上手に使いこなさないと、という感じですね



shun-inagaki 3:05 PM

デコード問の解空間が小さければ、いけますかね？



you0708 3:06 PM

どうなのでしょう。まあでも大事な部分は RC4 だったり AES だったりするの



shun-inagaki 3:14 PM

やっぱ厳しいですね.....

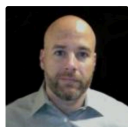


you0708 3:35 PM

では別案を採用するということで、Daserf をベースに課題案作ってみます。

Tick/Daserf

日本国内で数年前から発生していた標的型攻撃



Jon DiMaggio
View Profile

Symantec Official Blog

Tick cyberespionage group zeros in on J

Compromised websites and spear-phishing emails used to infect

By: Jon DiMaggio SYMANTEC EMPLOYEE

Created 28 Apr 2016 0 Comments 简体中文, 繁體中文, 日本語, 한국어



<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。

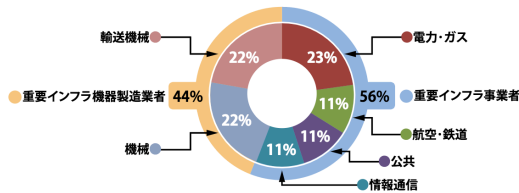


図1 ラックが対応した標的型攻撃事案のターゲット組織

http://www.lac.co.jp/security/report/pdf/20160802_cgview_vol12_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

```
http://27921119714/mttxlqy.php?id=0f19871r2&vpsx=GvUnX8Hh...
http://27921119714/jamdtsg.php?id=900c9554&toya=G0u577...
http://27921119714/atmdkno.php?id=a5287170&mngc=G0M577...
http://27921119714/cvowkfe.php?id=0a4c0111&phth=GvUnX8Hh...
http://27921119714/pvmdmvk.php?id=0d9671d1&ncwj=G0B577...
http://27921119714/jhmdthc.php?id=9ff56658&drkg=GH4571...
http://27921119714/zmmdmtd.php?id=496b5176&weli=GH577...
http://27921119714/gumsab.php?id=d9e80556&mdjv=GHF577...
http://27921119714/hwmdepg.php?id=6caad919&hckj=G0M577...
http://27921119714/wcmdawm.php?id=d725844c&szkl=G0M577...
http://27921119714/zpmdvgp.php?id=8de5e77b&gqxs=G0h577...
http://27921119714/limdbzk.php?id=28fae191&zicz=G0u577...
http://27921119714/ubmdowp.php?id=f6709445&fbba=Gc0577...
http://27921119714/nrmdrvv.php?id=91bef23f&jcfq=Gch577...
http://27921119714/rfmdqpr.php?id=64014216&zsgj=Gcd577...
http://27921119714/jtmdkdf.php?id=0cd8d416&ibxt=GdM577...
http://27921119714/wumdpql.php?id=8274b1M2&lfe1=GdM577...
http://27921119714/wdmdled.php?id=2336c11f&sjog=G0T577...
http://27921119714/vamd wok.php?id=b697b117&pnat=Gdx577...
```

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], 0FFFFFFFh
004188B7 94C      jz     loc_418B39
004188BD 94C      push   2                ; dwMoveMethod
004188BF 950      push   0                ; lpDistanceToMoveHigh
004188C1 954      push   0FFFFFFE16h     ; 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