contagio

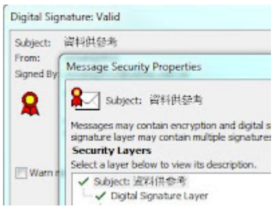
malware dump

Home

Mobile and print friendly view |

TUESDAY, OCTOBER 16, 2012

CVE-2012-1535 Sep.9, 2012 "房號表.doc - Data for Reference.doc" and Taidoor trojan sample set for signature development



Digital Signature: Valid

Subject: 資料供參考

From:

Signed By

Message Security Properties

Subject: 資料供參考

Messages may contain encryption and digital s
signature layer may contain multiple signatures

Security Layers

Select a layer below to view its description.

✓ Subject: 資料供參考

✓ Digital Signature Layer

□ Warn m

As promised, here is one sample of CVE-2012-1535 that you can use to follow the exploit analysis in the previous post CVE-2012-1535 Adobe Flash Player Integer Overflow Vulnerability Analysis by Brian Mariani & Frédéric Bourla. It is from September 9, 2012, I have one from October, which I will post shortly as well. If you are not interested in the exploit, you can use the Taidoor payload plus 18 other Taidoor binaries to develop your own signatures for this trojan or test your AV.

This message was sent to Taiwan government and is digitally signed with a valid signature. I am not sure if the signature is obtained for a fake account or the account is hijacked, this is why I am not posting the email address. If you work for TW government, you can ask for it. There was also a PDF attached with a personally identifiable information (full application) of an applicant for International Cooperation and Development Fund (Taiwan) - Women Development program. It is not included in this post. I assume it was stolen earlier as well.

CVE #

CVE-2012-1535

Unspecified vulnerability in Adobe Flash Player before 11.3.300.271 on Windows and Mac OS X and before 11.2.202.238 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted SWF content, as exploited in the wild in August 2012 with SWF content in a Word document.

Download

Download (email me if you need the password)

- http://contagio.deependresearch.org/files/CVE/CVE-2012-0158_Taidpoor_malware_2C199988A121B60818FA7D534E6C67B4.zip (with Taidoor 40d79d1120638688ac7d9497cc819462)
- http://contagio.deependresearch.org/files/bin/Taidoor_tar.zip (tar archive contents with taidoor binary desktop.ini 6D6B797C99A11B066746948EB1EF4AA8 and shortcut to it)

Download 18 Taidoor binaries for signature development and research (email me if you need the password)

List of files

CVE-2012-1535 2C199988A121B60818FA7D534E6C67B4 房號表.doc

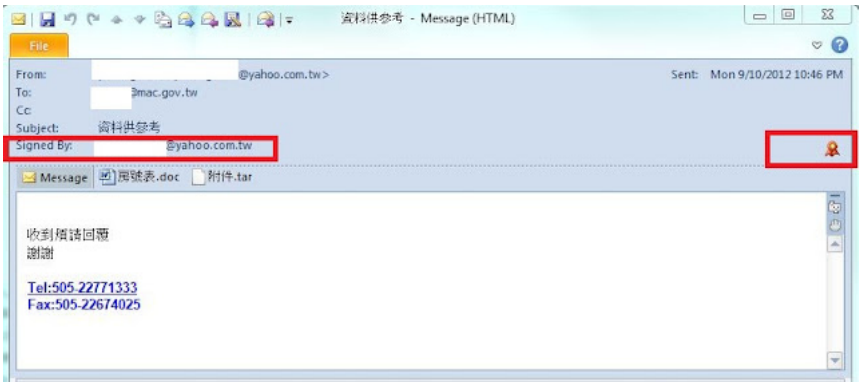
Taidoor binaries for research

0D0F38981E6CF09E82D6E55388A6F478
22E4F5AF13E6142E1623DFBFA05B5AD4
30768B6024557DDA108B648DC535A5EB
40D79D1120638688AC7D9497CC819462
6841A2C4EA247786241F5AB07050E3A4
7B806E6BFC75155EF8FC3DDC9D2B0113
83A0609EE10D87A66278CCCEBF8C6449
A47BDA32F159DEFC594D41526C65130A
A5E11557AF48B26279B430E1D1249A3B
AC3B1CABE39BCBD517B5E24A2320360F
C07F9E0C804D8972E5D8D3F000DF5CDE
C26178BF39160BF7B362A83D15F808E4
CC2C80F5472EC9A915452BB6F023063C
D5AB3E5DFC80FD03C789C5733B666B9C
E8CDFD82AA1F52F3CD2BBD845E17B354
F1A1C8900829185C5367C57A26453A13
F61056E724133467EDF61DECE1C9AEBF
F99554368B58D31F3AA389E81A98A95A

Payload information

40d79d1120638688ac7d9497cc819462 Taidoor WPFFontCache_v0400.exe (in Word)
6d6b797c99a11b066746948eb1ef4aa8 Taidoor desktop.ini in the tar file (appears malformed)

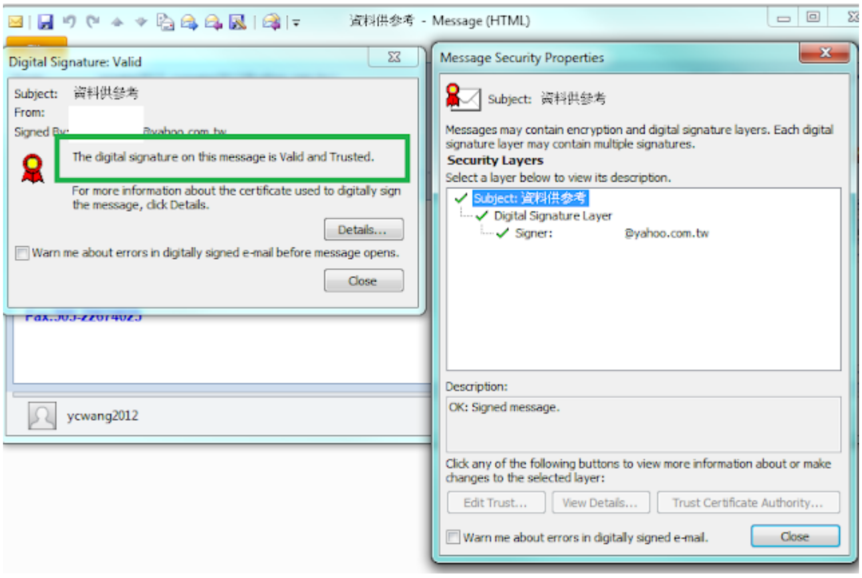
The message sent to TW government
Digitally signed



From: [redacted]@yahoo.com.tw> Sent: Mon 9/10/2012 10:46 PM
To: [redacted]@mac.gov.tw
Cc:
Subject: 資料供參考
Signed By: [redacted]@yahoo.com.tw

收到煩請回覆
謝謝

Tel:505-22771333
Fax:505-22674025



Digital Signature: Valid

Subject: 資料供參考
From: [redacted]
Signed By: @yahoo.com.tw

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

□ Warn me about errors in digitally signed e-mail before message opens.

Message Security Properties

Subject: 資料供參考

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

✓ Subject: 資料供參考
✓ Digital Signature Layer
✓ Signer: [redacted]@yahoo.com.tw

Description:

OK: Signed message.

Click any of the following buttons to view more information about or make changes to the selected layer:

□ Warn me about errors in digitally signed e-mail.

房號表.doc

Data for reference

Table of the room number '

Receive please reply

Thank you

Tel :505-22771333

Fax :505-22674025

From: xxxxxxxx [mailto:xxxx@yahoo.com.tw]

Sent: Monday, September 10, 2012 10:46 PM

To: xxxxxxxx@mac.gov.tw

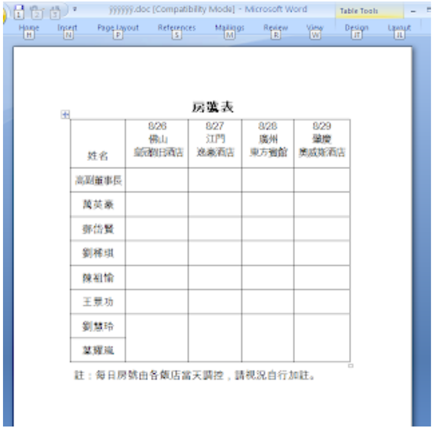
Subject: 資料供參考

收到煩請回覆

謝謝

Tel:505-22771333

Fax:505-22674025



房號表

姓名	8/26 佛山 皇冠假日酒店	8/27 江門 逸豪酒店	8/28 廣州 東方賓館	8/29 肇慶 美成斯酒店
高副董事長				
萬英豪				
張岱賢				
劉椿琪				
陳祖愉				
王景功				
劉慧玲				
葉耀嵐				

註：每日房號由各飯店當天調控，請視況自行加註。

lure 2C199988A121B60818FA7D534E6C67B4

#1 2C199988A121B60818FA7D534E6C67B4

Payload - Trojan Taidoor / Simbot embedded in the Word document and inside the tar archive (desktop.ini (Taidoor 9 / 43 Virustotal) file with a PDF (Virustotal) and a shortcut file (`C:\WINDOWS\system32\cmd.exe /c desktop.ini`)

Virustotal for 5387ad3225657f8857ddeaf70346722b1ef232beff3d74a9bf8d31738fc9c59a

Created files locations
Local Settings\Temp\ÿÿÿÿÿÿ.doc <decoy
Local Settings\Messenger.exe < file name varies
Local Settings\NetDDEdsdm.exe
Local Settings\WPFFontCache_v0400.exe
Local Settings\Temp\~dfds3.reg

Artifacts locations
Doctor Watson files due to the initial crash
Local Settings\History\History.IE5\MSHist012012101420121015\index.dat
Local Settings\Temp\65824578.od
Local Settings\Temp\dw.log
Local Settings\Temp\Word8.0\ShockwaveFlashObjects.exd
Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
\Temporary Internet Files\Content.MSO\26F7849B.wmf

Created files:
MD5:

Messenger.exe	40d79d1120638688ac7d9497cc819462 << file name varies!
NetDDEdsdm.exe	40d79d1120638688ac7d9497cc819462
WPFFontCache_v0400.exe	40d79d1120638688ac7d9497cc819462
~dfds3.reg	eeda7daba8d3329e33a9d2b0e56f4f80

Sha256

5387ad3225657f8857ddeaf70346722b1ef232beff3d74a9bf8d31738fc9c59a WPFFontCache_v0400.exe
7cb6182a8972a6aae9511f9d23ef6414a30bfb24fa8f1926d3cd81072414f75d ~dfds3.reg

Artifacts
26F7849B.wmf
66121875.od
dw.log
index.dat
ShockwaveFlashObjects.exd

ssdeep:
384:yPNY1M5Zni1HHl2EqVZqbS0hVYk4h5t6Dla:kEq8l2nqbXYP60,"Messenger.exe"

Traffic
Process ID: 2744 (svchost.exe)
Process doesn't appear to be a service

```
PID      Port        Local IP              State                  Remote IP:Port
2744 TCP 1229   172.16.253.132  ESTABLISHED  211.234.117.141:443
                               | Frames  Bytes |  | Frames  Bytes |  | Frames  Bytes |
211.234.117.141     <-> 172.16.253.132        1000    103328     862      51720     1862     155048

  Active Connections
  Proto  Local Address          Foreign Address        State          PID
  TCP    172.16.253.132:1375    211.234.117.141:443    FIN_WAIT_2     2744
  C:\WINDOWS\system32\WS2_32.dll
  C:\WINDOWS\system32\WININET.dll
  [svchost.exe]
```

WHOIS Source: APNIC
IP Address: **211.234.117.141**
Country: Korea, Republic Of
Network Name: KIDC-KR
Owner Name: LG DACOM KIDC
From IP: 211.234.96.0
To IP: 211.234.127.255
Allocated: Yes
Contact Name: Host Master
Address: 11F, KTF B/D, 1321-11, Seocho2-Dong, Seocho-Gu,, Seoul, Korea, 137-857
Email: hostmaster@nic.or.kr
Phone: +82-2-2186-4500
Fax: +82-2-2186-4496

```
GET /apzsr.php?id=021793111D309GE67E HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 211.234.117.141:443
Connection: Keep-Alive
Cache-Control: no-cache
```

```
strings_~dfds3.reg
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"WPFFontCache_v0400"="C:\\Documents and Settings\\Laura\\Local Settings\\WPFFontCache_v0400.exe"
```

Email Headers

SAMPLE #1 2C199988A121B60818FA7D534E6C67B4

```
Microsoft Mail Internet Headers Version 2.0
Received: from mse99.trade.gov.tw ([172.16.2.4]) by mail93.trade.gov.tw over TLS secured channel with Microsoft
SMTPSVC(6.0.3790.4675);
  Tue, 11 Sep 2012 10:46:25 +0800
Received: from AntiSpam.trade.gov.tw (antispam.trade.gov.tw [172.17.1.4])
 by mse99.trade.gov.tw with ESMTP id q8B2kJNZ080932
 for <xxxxxxxxxx@trade.gov.tw>; Tue, 11 Sep 2012 10:46:19 +0800 (GMT-8)
 (envelope-from xxxxxxx@yahoo.com.tw)
Received: from nm26-vm9.bullet.mail.sg3.yahoo.com (nm26-vm9.bullet.mail.sg3.yahoo.com [106.10.151.120])
 by AntiSpam.trade.gov.tw with SMTP id q8B2kCCb051478
 for <smh@trade.gov.tw>; Tue, 11 Sep 2012 10:46:12 +0800 (CST)
 (envelope-from xxxxxxxxxxx@yahoo.com.tw)
Received: from [106.10.166.116] by nm26.bullet.mail.sg3.yahoo.com with NNFMP; 11 Sep 2012 02:46:12 -0000
Received: from [106.10.167.238] by tm5.bullet.mail.sg3.yahoo.com with NNFMP; 11 Sep 2012 02:46:10 -0000
Received: from [127.0.0.1] by smtp211.mail.sg3.yahoo.com with NNFMP; 11 Sep 2012 02:46:10 -0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com.tw; s=s1024; t=1347331570;
bh=y/fTGjKrz3P9wnnVOmsuyivYegUymx1m+pNZIqSI8io=; h=X-Yahoo-Newman-Id:X-Yahoo-Newman-Property:X-YMail-OSG:X-Yahoo-
SMTP:Received:Message-ID:From:To:Subject:Date:MIME-Version:Content-Type:X-Priority:X-MSMail-Priority:X-Mailer:X-MimeOLE;
b=BUNM174C2z5YUcyGfAKTAir+opr4A/fP53RmctXSWVtyJjmanA9UACeePVMrBEal78LLYCM9Rsxwhilp1zL6WIllyIrpr0QkSCwH0cviuMoVeHcbOn+NYjedOkZW4gU2
7E0cUSoiCJcX+IB/S698snOtUrF1P7Myy0DbOpoC4=
X-Yahoo-Newman-Id: 538238.79310.bm@smtp211.mail.sg3.yahoo.com
X-Yahoo-Newman-Property: ymail-5
X-YMail-OSG: M_hRw4wVM1lKJVKy3cN._hIFgwq7ygzEDXdVecwWndt0GCK
 UYyfTw_pZb5Zl.vKdwNgbVhgbvIYW6Apbi_6qrta83ynjAQU9gosALflRvlj
 1P8cG27uA3C2TQSGhNbASyznBE8G0iD9IzO6Bwp16HtZbJU9pbRWkBz79ULj
 1A6OCOnKOfqJZPy9sMPeDz8HRIY1iFT1wyTMvrnczltjCk2LPCriCnNIHQx.
 wiQkHjRgleWGaSE7ttC2ZV9RIjPQgh0.g9uo0UZ.LlmAUh7kRVP9oOvHmPqJ
 P5q_Gzc8aPC2akubsC8IPycCSta_7nCtl82o5t59LOqP5n0paxFa_0.w2tRF
 leWS4Pxjzw6JzmyVyYOTcdR9kVLCcXwYd7VxVUtmczoLB8XfFiACzeAQ0WBn
 KpUY5KWwDe4FklBAB1uQ3F9i3OPdaNw0K
X-Yahoo-SMTP: QFan6h2swBBkcpPdQXIiwXg08TmA4BU-
Received: from SFGDSGSGFDSG (xxxxxxxxx@111.254.231.18 with login)
        by smtp211.mail.sg3.yahoo.com with SMTP; 10 Sep 2012 19:45:40 -0700 PDT
Message-ID: <14FD634A91254F6D81F309B6AE0D96D2@SFGDSGSGFDSG>
From: xxxxxxxxx@yahoo.com.tw>
To: xxxxxxxx@mac.gov.tw>
Subject: =?big5?B?uOquxqjRsNGm0g==?=
Date: Tue, 11 Sep 2012 10:45:37 +0800
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/x-pkcs7-signature";
 micalg=SHA1;
 boundary="----=_NextPart_000_00F2_01CD900A.93FD5BE0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5931
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.6109
X-DNSRBL:
X-MAIL: xxx.trade.gov.tw q8B2kJNZ080932
Return-Path: xxxxxxxxxxyahoo.com.tw
X-OriginalArrivalTime: 11 Sep 2012 02:46:25.0984 (UTC) FILETIME=[A3043C00:01CD8FC7]
```

Automatic scans

Virustotal for 5387ad3225657f8857ddeaf70346722b1ef232beff3d74a9bf8d31738fc9c59a

SHA256: 5387ad3225657f8857ddeaf70346722b1ef232beff3d74a9bf8d31738fc9c59a
SHA1: e4a5517ed0626677a31f123446403dd1e79afca4
MD5: 40d79d1120638688ac7d9497cc819462
File size: 32.0 KB (32768 bytes)
File name: WPFFontCache_v0400.exe
File type: Win32 EXE
Tags: peexe armadillo
Detection ratio: 20 / 44
Analysis date: 2012-10-14 21:16:36 UTC (1 day, 4 hours ago)

Antivirus Result Update
AVG Generic29.AHPF 20121014
BitDefender Gen:Trojan.Heur.RP.cq0@ayoZefab 20121014
Emsisoft Backdoor.Win32.Simbot!IK 20120919
ESET-NOD32 a variant of Win32/Injector.UQP 20121014
F-Secure Gen:Trojan.Heur.RP.cq0@ayoZefab 20121003
GData Gen:Trojan.Heur.RP.cq0@ayoZefab 20121014
Ikarus Backdoor.Win32.Simbot 20121014
Kaspersky Trojan.Win32.Inject.elqk 20121014
Kingsoft Win32.Troj.Inject.(kcloud) 20121008
McAfee-GW-Edition - 20121014
Microsoft Backdoor:Win32/Simbot.gen 20121014
MicroWorld-eScan Gen:Trojan.Heur.RP.cq0@ayoZefab 20121014
Norman W32/Obfuscated_JA 20121014
nProtect Trojan/W32.Inject.32768.CG 20121014
Panda Suspicious file 20121014
PCTools Trojan.Taidoor 20121014
Sophos Mal/Simbot-B 20121014
Symantec Trojan.Taidoor!gen1 20121014
TrendMicro BKDR_SIMBOT.SMAZ 20121014
TrendMicro-HouseCall BKDR_SIMBOT.SMAZ 20121014
ViRobot Backdoor.Win32.Simbot.32768 20121014

https://www.virustotal.com/file/950aef9e49da2f64cbf48f3c3e31545f463686989ed75c332168fdfc841bf26d/analysis/1350361985/
SHA256: 950aef9e49da2f64cbf48f3c3e31545f463686989ed75c332168fdfc841bf26d
SHA1: e519986529723c74d93efe8441ea42985529805b
MD5: 6d6b797c99a11b066746948eb1ef4aa8
File size: 36.1 KB (36976 bytes)
File name: desktop.ini
File type: Win32 EXE
Detection ratio: 9 / 43
Analysis date: 2012-10-16 04:33:05 UTC (0 minutes ago)
Additional information
Antivirus Result Update
Agnitum Suspicious!SA 20121014
AVG Suspicion: unknown virus 20121016
Comodo UnclassifiedMalware 20121016
ESET-NOD32 a variant of Win32/Injector.XDH 20121015
Ikarus Virus.Win32.Patched 20121016
Kingsoft Win32.Troj.Sasfis.(kcloud) 20121008
Norman W32/Obfuscated_JA 20121015
Symantec WS.Reputation.1 20121016
TrendMicro-HouseCall TROJ_GEN.F47V0911 20121016

Posted by Mila at 1:33 AM Tags: CVE-2012-1535, taidoor

1 comment:

Quetzalcoatl November 9, 2012 at 7:40 PM

All news about malware you can to find heere. :) http://malware-source.com/

Reply

Enter Comment

Newer Post Home Older Pos

Subscribe to: Post Comments (Atom)

Home

Powered by Blogger.